UNIVERSIDAD NACIONAL DE LA MATANZA

ESCUELA DE POSGRADO

MAESTRIA EN INFORMÁTICA

TESIS DE MAESTRÍA

Título de Tesis:

ASEGURAMIENTO DE AUTENTICACIÓN EN INTERNET DE LAS COSAS

Autor: Ing. Pablo Hernán Pomar

Director: Mg. Ing. Jorge Esteban Eterovic

Buenos Aires, *octubre de 2019*

Agradecimientos

En primer lugar, quería agradecer a toda mi familia. Mi esposa Melina y a mis hijas Milena y Carolina, fundamentales para que este trabajo sea posible. Me apoyaron en todo momento para que lo hiciera y cedieron de "su" tiempo para que yo tuviera el "mío" para realizarlo. Cada vez que las necesité, ya sea un mate de madrugada o un rato a solas, no dudaron un solo instante en dármelo.

A mis padres, Elsa y Leopoldo, que desde el cielo guían mis pasos.

También quiero destacar el apoyo de mis suegros, Elena y Manuel, y cuñados Camila y Alejandro.

Desde el lado laboral y profesional, también agradecer a mis colegas por las palabras de aliento y la colaboración con los temas y dudas presentados y/o comentados.

Quisiera hacer llegar mi gratitud al tutor de la presente Tesis, Jorge, que siempre estuvo predispuesto a acompañarme en el desarrollo del trabajo.

(Página en blanco)

Resumen

Con el advenimiento de "Internet de las Cosas", comúnmente conocido como "*IoT*", del inglés "*Internet of Things*", se plantea un nuevo escenario dentro de las TICs[1], donde la gestión de la información, es decir cómo se obtiene, cómo se trata y fundamentalmente sus resultados impactarán en nuestra vida cotidiana.

Involucra diversas tecnologías de reciente aparición como *Big Data*[2], Redes de Sensores Inalámbricos, *Cloud Computing*[3], y otras ya más desarrolladas como la Criptografía Ligera y los mecanismos de Autenticación.

Internet de las Cosas generará nuevos productos y servicios, hará más eficiente el uso de recursos y permitirá actuar y comprender mejor el entorno.

Pero, como toda nueva tecnología, traerá aparejados nuevos riesgos para la seguridad y la privacidad de la información ya que se recopilará información sobre las actividades, costumbres, preferencias, etc. de los usuarios.

Esta situación genera desconfianza y, para reducirla, se deberán establecer conexiones entre entornos seguros y definir el uso que se hace con los datos recolectados.

Dentro de los entornos seguros, uno de los desafíos a resolver será cómo autenticar de manera confiable, robusta y ágil a quién acceda, recolecte, procese y utilice la información en este nuevo escenario.

Otro de los desafíos será cómo establecer estándares, de la industria o por cumplimiento de normativas, para el aseguramiento de esta tecnología.

[1] **TICs**: Siglas de Tecnologías de Información y Comunicación: Conforma el conjunto de recursos necesarios para manipular y/o gestionar la información: los ordenadores, los programas informáticos y las redes necesarias para convertirla, almacenarla, administrarla, transmitirla y encontrarla.

[2] **Big Data** representa los activos de información caracterizados por un volumen, velocidad y variedad tan altos que requieren una tecnología específica y métodos analíticos para su transformación en valor". Además, algunas organizaciones agregan una nueva V, veracidad para describirlo, revisionismo cuestionado por algunas autoridades de la industria. Las tres V (volumen, variedad y velocidad) se han ampliado a otras características complementarias del *big data*.
Presenta las siguientes características:

- Volumen: la cantidad de datos generados y guardados.
- Variedad: el tipo y naturaleza de los datos para ayudar a las personas a analizarlos y usar los resultados de forma eficaz. Los macro datos usan textos, imágenes, audio y vídeo.
- Velocidad: en este contexto, la velocidad a la cual se generan y procesan los datos para cumplir las exigencias y desafíos de su análisis.
- Veracidad: la calidad de los datos capturados puede variar mucho y así afectar a los resultados del análisis.
- Valor: los datos generados deben ser útiles, accionables y tener valor

[3] **Cloud Computing** es un conjunto de principios y enfoques que permite proporcionar infraestructura informática, servicios, plataformas y aplicaciones (que provienen de la nube) a los usuarios, según las soliciten y a través de una red

Abstract

With the advent of "Internet of Things", commonly known as "IoT", of the English "Internet of Things", a new scenario is proposed within the TICs, where information management, that is, how it is obtained, how It is about and fundamentally its results will impact our daily lives.

It involves several technologies of recent appearance such as Big Data, Wireless Sensor Networks, Cloud Computing, and other more developed such as Light Cryptography and Authentication mechanisms.

Internet of Things will generate new products and services, make the use of resources more efficient and allow the environment to act and understand better.

But, like all new technology, it will entail new risks for the security and privacy of information as information on activities, customs, preferences, etc. will be collected. of the users.

This situation creates distrust and, to reduce it, connections between secure environments must be established and the use made of the data collected must be defined.

Within the secure environments, one of the challenges to be solved will be how to authenticate in a reliable, robust and agile way who accesses, collects, processes and uses the information in this new scenario.

Another of the challenges will be how to establish standards, of the industry or for compliance with regulations, for the assurance of this technology.

Índice

Índice de Ilustraciones

Índice de Tablas

CAPITULO I – Contexto de la Investigación

(Página en blanco)

1. Fundamentación de la problemática

Internet de las Cosas todavía suena como una de esas palabras/frases de moda o futuristas que aún está demasiado lejos para pensar mucho en ella. Pero el *IoT* ya está presente y entre otras cosas, está cambiando nuestra salud, como construimos, como nos movemos y generando miles de millones de dólares en valor en múltiples sectores.

Pero no sólo hay que ver el lado económico de esta revolución tecnológica.

Estos dispositivos están sensando, capturando, comunicando y procesando información proveniente de muchos usuarios, poniendo en evidencia sus actividades y sus preferencias.

Del mismo modo, está poniendo en funcionamiento millones de equipos, con cierto nivel de cómputo en "la calle", con un mínimo control.

Según estadísticas del 2018 había 23.140 millones de dispositivos y para el 2025 este número se incrementará más de 3 veces (IoT Word on Line, 2019), como puede observarse en la siguiente ilustración.

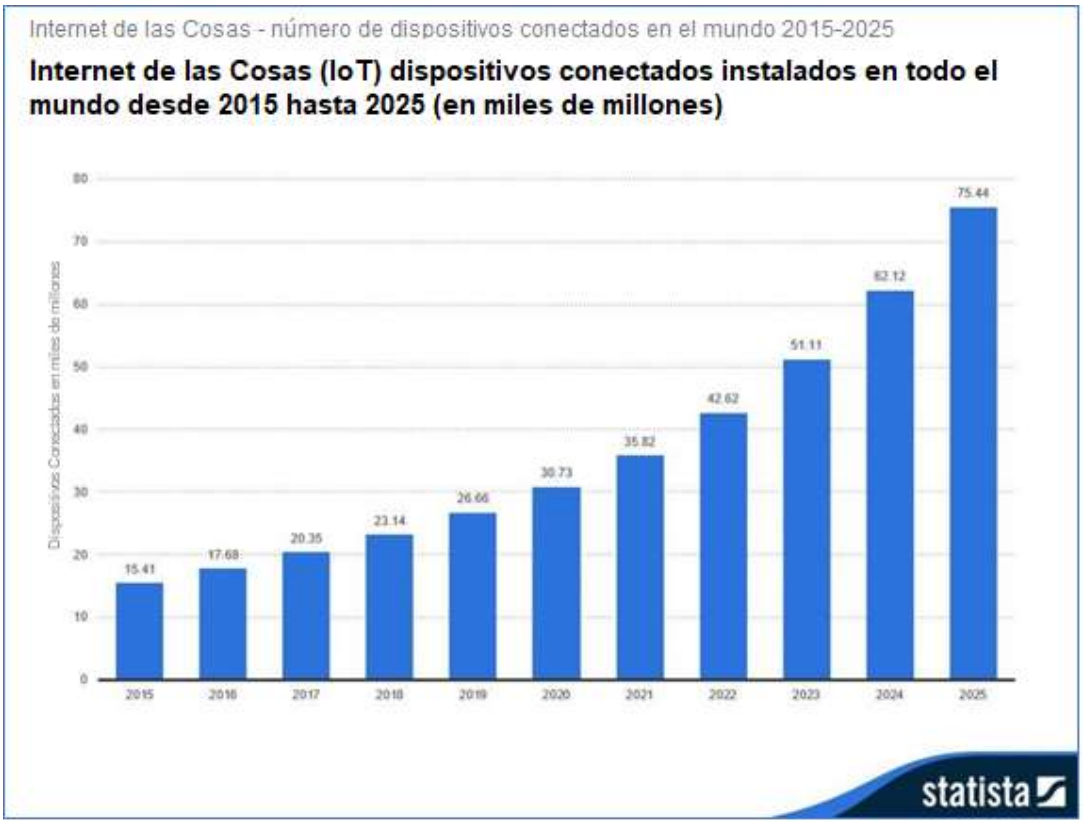


Ilustración 1 - Dispositivos conectados en el mundo 2015-2025
Fuente: https://www.iotworldonline.es/las-grandes-estadisticas-del-internet-de-las-cosas-iot/

Otra característica destacable es que estos dispositivos no están concentrados solamente en hacer más inteligentes a las ciudades, o conectar a los autos para darnos más seguridad en el manejo, también se incorporan a la moda (ropa y accesorios) y controlarán en aspectos de salud.

El abaratamiento de los costos también colabora en la "masificación" de los dispositivos, impulsando a que esta tecnología esté en todos los ámbitos, tal como lo representa la siguiente ilustración.

Ilustración 2 - Ámbito de IoT
Fuente: https://www.rfpage.com/wp-content/uploads/2017/11/Top-IOT-Platforms.jpg

En un estudio de *IoT Analytics* sobre 1600 proyectos empresariales sobre 10 segmentos principales que cubren aplicaciones en más de 70 países de todo el mundo, se destacan los siguientes datos (IOT Analytics, 2018), representados en la "ilustración 3".

Los casos de estudio de Internet de las Cosas que forman parte de las iniciativas de *Smart City*[4] conforman la mayor parte de los proyectos identificados (23%), seguidos de los proyectos implementados en entornos industriales (17%) y los proyectos que evolucionan alrededor de Edificios conectados (12%).

[4] **Smart City**: traducido como "Ciudad Inteligente". Una ciudad se puede definir como "inteligente" o como "inteligentemente eficiente", cuando la inversión social, el capital humano, las comunicaciones, y las infraestructuras, conviven de forma armónica con el desarrollo económico sostenible, apoyándose en el uso y la modernización de nuevas tecnologías (TIC), y dando como resultado una mejor calidad de vida y una gestión prudente de los recursos naturales, a través de la acción participativa y el compromiso de todos los ciudadanos.

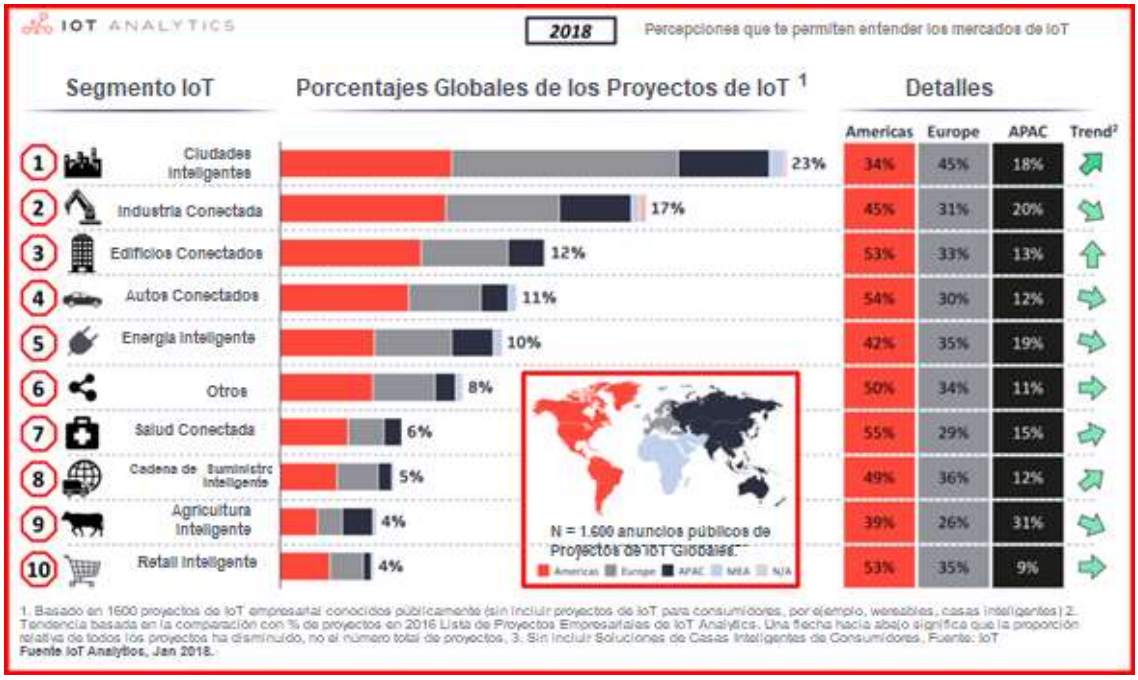


Ilustración 3 - Proyectos de IoT por Segmentos durante el 2018

Fuente: https://iot-analytics.com/wp/wp-content/uploads/2018/01/Overview-IoT-Enterprise-Projects-List-2018-Edit.png

Esta exposición de los dispositivos *IoT* en los hogares, sobre las mismas personas (por el uso de "*wereables*"[5]) y oficinas están captando la atención de los cibercriminales.

El objetivo de éstos es captar a dichos dispositivos para actividades ilícitas relacionados, en su mayoría, a formar parte de *botnets*[6] para la generación de ataques de "denegación de servicio"[7] o realizar minería de criptomonedas[8].

[5] **Wereables**: La tecnología vestible (del inglés wearable technology), tecnología corporal, ropa tecnológica, ropa inteligente, o electrónica textil, son dispositivos electrónicos inteligentes incorporados a la vestimenta o usados corporalmente como implantes o accesorios que pueden actuar como extensión del cuerpo o mente del usuario.
Los dispositivos vestibles como los monitores de actividad son un buen ejemplo del Internet de las cosas, puesto que cosas como la electrónica, software, sensores y conectividad son mecanismos que permiten a los objetos intercambiar información a través de Internet con un fabricante, operador u otros dispositivos conectados, sin necesitar de la intervención humana.

[6] **Botnet** es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota. Entre los usos más comunes están:

- Ataques de denegación de servicio distribuidos (DDoS)
- Envío de Spam
- Minería de Bitcoins
- Robo de Bitcoins

[7] **Ataque de Denegación de Servicio** (también conocido como ataque DoS) es un intento malicioso de hacer que un sitio o una aplicación web no estén disponibles para los usuarios legítimos saturando de forma intencionada la infraestructura que soporta el sitio con un enorme volumen de tráfico falso, hasta el punto de que el sitio no puede procesar más solicitudes o lo hace muy lentamente

[8] **Minería de Criptomonedas**: En el mundo de las criptomonedas el dinero no se crea, sino que se descubre. A este proceso se lo conoce como minería.
Los mineros obtienen como recompensas criptomonedas cada cierta cantidad de tiempo, una vez que se resuelve un problema matemático.

Según una investigación sobre el mercado de Reino Unido (IoT News, 2019), los ataques de *IoT* pueden costar a la economía del Reino Unido más de 1.000 millones de libras al año debido a medidas de seguridad laxas.

Dicho informe menciona que, en las organizaciones británicas en industrias críticas, como la salud, el transporte y la manufactura, los ataques contra equipos de *IoT* causaron pérdidas (con un promedio de £ 244,000) debido a que los ciberdelincuentes están encontrando cada vez nuevas y creativas maneras de convertir la dependencia tecnológica en su propia ganancia nefasta.

Distintas organizaciones del orden, tales como el *FBI* e *Interpol* (IoT News, 2019) alertan sobre los peligros de conectar dispositivos a Internet.

Empresas privadas de seguridad, como organizaciones estatales relacionadas con el tema de seguridad están analizando estudios y un seguimiento de estas alertas, de manera de contrarrestarlas.

Según estudios de la empresa F-Secure en su informe anual 2018 (F-Secure, 2019), desde el 2002, se han incrementado la cantidad de problemas de seguridad asociados a *IoT*.

Tal como es presentado en la siguiente tabla, durante varios años la cantidad de ataques estuvo estable respecto a la cantidad hasta “pegar el salto” en el 2018

Año	Cantidad
2002	1
2008	1
2009	1
2011	1
2014	3
2015	2
2016	5
2017	5
2018	19

Tabla 1 - Tabla comparativa Ataques/años
Fuente: Informe “Iot threat landscape Old hacks, new devices” empresa F-Secure

En la actualidad se puede conseguir hardware especializado para este tipo de procesos, el cual es muy costoso y lleva tiempo recuperar la inversión. La idea de los atacantes es usar hardware "capturado" para ponerlo a funcionar como propio y resolver los problemas matemáticos propuestos y obtener dichas recompensas.

Según el informe, una buena parte de los mismos se encuentra relacionada con claves débiles o "por defecto", como queda plasmado en la siguiente ilustración:

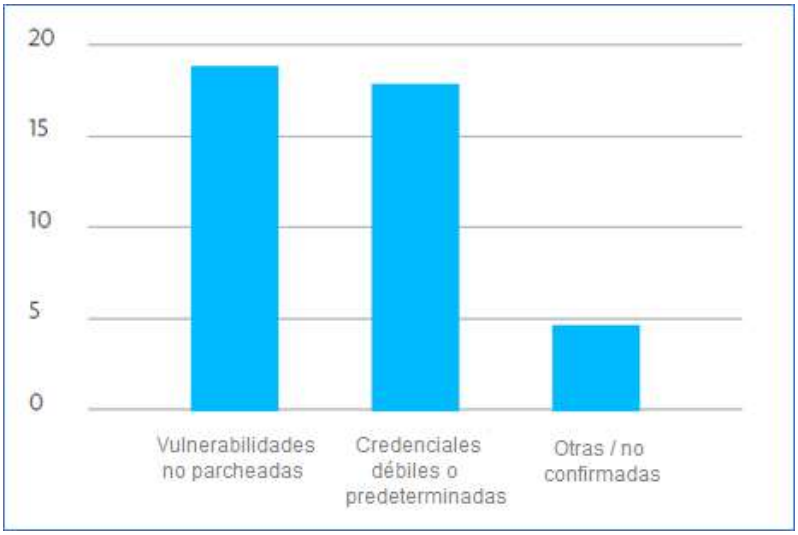


Ilustración 4 - Tipos de vulnerabilidades
Fuente: Informe "Iot threat landscape Old hacks, new devices" empresa F-Secure

Analizando con un poco más de profundidad el tipo de ataques en el tiempo, queda en evidencia que prevalecen, todavía, los tipos de ataques relacionados con credenciales[9].

Cualquier aparato presentado en estos últimos años ya es "inteligente" por definición e incluye interconexión con otros dispositivos e intercambio de información para prestar más y mejores servicios, como puede encontrarse en cada feria *Consumer Electronic Show*[10], realizada anualmente en Las Vegas, donde son presentados los diferentes dispositivos tecnológicos nuevos.

Como lo ha podido demostrar la historia, los avances tecnológicos, además de traer beneficios a los usuarios, tiene aparejados riesgos y responsabilidades (en este último caso al menos debería).

Lamentablemente, a esta situación se le adiciona que, pueden representar un importante problema en términos de seguridad.

Para poder "graficar" este problema, serán citados algunos ejemplos conocidos y/o divulgados, de diferentes ámbitos:

[9] **Credenciales**: Conjunto formado por nombre de usuario y contraseña, por lo general, utilizado para autenticar a un usuario.
[10]**Consumer Electronic Show:** https://www.ces.tech

1) **Dispositivos de consumo conectados a Internet utilizados como una red de robots (thingbots).** (Infobae.com, 2014)

   Durante el 2014 aparecieron diferentes artículos sobre el uso de distintos dispositivos hogareños para formar "*botnets*". Por medio de estas se realizaron diferentes tipos de ataques.

   Un famoso ataque de estas características, descripto por la empresa Proofpoint fue realizado por 100.000 electrodomésticos "inteligentes", entre los cuales se destacaba televisores y (al menos) una heladera que enviaron 750.000 correos masivos (*spam*[11]). Las vulnerabilidades presentadas de estos equipos eran el uso de contraseñas por defecto, que no habían sido cambiadas, y otros errores de configuración de los equipos.

2) **Un hacker roba en un casino de un hotel de Londres colándose a través de una pecera** (Diaro El Mundo, 2018)

   Por medio de un termostato que regula la pecera del casino, conectado a internet, un hacker pudo robar una base de datos de clientes selectos, con consumos importantes e información privada de todo tipo.

   Todas las peceras estaban conectadas y se ajustan según la temperatura externa o la hora o el estado de los peces, siendo gobernadas por un sistema automático. El ingreso a la red fue por medio de un termostato conectado a dicha red.

3) **Asistente Virtual Amazon Alexa nos espía…** (Barnes, 2017)

   Si un atacante tenía acceso físico al dispositivo le era posible instalar *malware*[12] en el asistente personal del hogar sin dejar rastro. Una vez que eso sucediera, el dispositivo podría ser monitoreado desde cualquier parte del mundo. Este fue el primer ejemplo

[11] **Spam**: Los términos correo basura, correo no solicitado y mensaje basura hacen referencia a los mensajes no solicitados, no deseados o con remitente no conocido (o incluso correo anónimo o de falso remitente), habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina *spamming*. La palabra *spam*, proviene de la época de la Segunda Guerra Mundial, cuando los familiares de los soldados en guerra les enviaban comida enlatada; entre las que se encontraba una carne enlatada llamada "spam", que en los Estados Unidos era y sigue siendo muy común. Este término comenzó a usarse en la informática décadas más tarde al popularizarse, gracias a un sketch de 1970 del grupo de comediantes británicos Monty Python, en su serie de televisión Monty Python's Flying Circus, en el que se incluía spam en todos los platos.

[12] **Malware**: El malware, en inglés, *malicious software*, programa malicioso, o programa maligno (también llamado *badware*, código maligno, software maligno, software dañino o software malintencionado) hace referencia a cualquier tipo de software maligno que trata de afectar a una computadora, a un teléfono celular u otro dispositivo. Se considera un tipo dañino de software si es destinado a acceder a un dispositivo sin el conocimiento del usuario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

exitoso de un atacante que obtiene acceso remoto al sistema de altavoces inteligentes de Amazon. También fue una vista previa deslumbrante de los peores escenarios que los consumidores podrían enfrentar al conectar sus aparatos a Internet.

La pregunta que surgió luego de la situación descripta fue: ¿Quién compraría un dispositivo inteligente para el hogar si pudiera convertirse en una "intervención telefónica"?

Por estas fallas encontradas, el dispositivo fue completamente rediseñado con una nueva arquitectura interna para 2018.

4) **Hackeo de semáforos de control de tráfico.** (Diario Clarin, 2014)

En junio de 2014, un experto argentino en seguridad informática, Cesar Cerrudo, pudo demostrar el acceso a los sistemas de control de tránsito y cambio de valores de los semáforos (de rojo a verde y viceversa) de ciudades como Washington DC, San Francisco y New York al encontrar que la información que "viaja" entre los sensores de tráfico no es encriptada y, obviamente, dicha vulnerabilidad puede ser explotada.

5) **Hackeo remoto de la computadora de automóviles.** (Chris Valasek, 2015)

En julio de 2015 los hackers Chris Valasek y Charlie Miller demostraron, por medio de videos y con publicaciones de *papers*, como pudieron tomar el control, de manera remota – vía Internet - de la computadora de un vehículo Jeep Cherokee, modelo 2014, cuando éste estaba en movimiento. El ataque se basó en la explotación de una vulnerabilidad "0-day"[13] que tenía el sistema UConnect de la computadora de abordo. En dicho vehículo pudieron:

- realizar cambios de velocidad,
- controlar los frenos,
- controlar la dirección,
- utilizar la radio
- manejar la transmisión, entre otras.

[13] **Vulnerabilidad "0-day"**: Una nueva vulnerabilidad para la cual no se crearon parches o revisiones, y que se emplea para llevar a cabo un ataque. El nombre 0-day (día cero) se debe a que aún no existe ninguna revisión para mitigar el aprovechamiento de la vulnerabilidad

Producto de esta demostración Fiat Chrysler llamó a revisión a 1,4 millones de vehículos afectados en EEUU para solucionar el problema de seguridad evidenciado.

6) **Ataque de Denegación de Servicios Distribuida (DDoS) al Servicio DNS provisto por la empresa Dyn deja fuera de servicio a toda la costa este de los Estados Unidos** (Wired, 2016)

Este ataque, conocido como el mayor ataque de *DDoS*[14] de la historia. Fue perpetrado por una *botnet* conocida como "Mirai"[15], cuyo código se había hecho público, que infectó a los dispositivos de Internet de las Cosas (entre los "participantes" se encontraban cámaras web, reproductores de video, enrutadores, etc.) con *malware* en todo el mundo. Una vez infectados, esos dispositivos conectados a Internet se convierten en parte de un ejército de *botnets*, conduciendo el tráfico malicioso hacia un objetivo determinado. En este caso había sido a la empresa Dyn, encargada de proveer el servicio de *DNS*[16].

El ataque forzó la desconexión de más de 100 sitios web (Twitter, Spotify, Netflix, Amazon, GitHub, PayPal, etc.) por varias horas. El mismo fue realizado en tres "oleadas" que involucraron a más de 10 millones de direcciones *IP*[17] que generaron un tráfico superior a 1 Terabits/segundo.

7) **Apagón forzado en Ucrania** (ESET, 2016)

El 23 de diciembre de 2015, la distribución de energía en Ucrania fue afectada por un ataque que interrumpió el servicio de una gran cantidad de usuarios durante varias horas.

[14] **DDoS**: *Distributed Denial of Service*. Traducido como "ataque de denegación de servicio distribuido". Es llevado a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino.

[15] **Mirai**: Malware para el control de *botnet* desarrollado sobre el código fuente filtrado de Gafgyt. Se popularizó cuando su código fue publicado en Github en 2016.
El desarrollo colaborativo de la amenaza la hizo mucho más potente. Originalmente, 61 combinaciones únicas de credenciales utilizadas para infecciones, utilizadas para acceder a distintos equipos que tenían credenciales por defecto.

[16] **DNS**: El sistema de nombres de dominio (*Domain Name System*) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

[17] **IP**: La dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, teléfono inteligente) que utilice el protocolo o (*Internet Protocol*), que corresponde al nivel de red del modelo *TCP/IP*.

Los piratas informáticos usaron el troyano[18] "*BlackEnergy"* para acceder al sistema de gestión de la distribución de energía y fueron así capaces de emitir comandos de interrupción del servicio, borrar y sobrescribir datos del sistema y realizar operaciones de apagado

Requerimientos y Retos de Seguridad

Un estudio realizado en el 2014, que a pesar de ser "obsoleto" puede considerarse como representativo, por Hewllet Packard (ComputerWorld, 2014) realizado sobre 10 tipos de dispositivos *IoT* más populares y/o frecuentes describió que se encontraron 250 vulnerabilidades (muchas de ellas severas) que permitirían realizar ataques de Denegación de Servicio y *Cross Site Scripting (XSS)*[19]. Además, mencionaba las siguientes características:

- El 90% de los dispositivos recolectaban algún tipo de dato personal
- El 80% de los dispositivos no solicitaba contraseñas con complejidad y longitud suficiente
- El 70% de los dispositivos permitían al atacante identificar cuentas de usuarios válidas realizando enumeraciones.
- El 70% de los dispositivos utilizaron servicios de red sin encripción.
- 6 de cada 10 dispositivos tenían interfaces de usuario vulnerables a *XSS* y con credenciales débiles.

Los datos de dicho informe se encuentran graficados en la próxima ilustración

[18] **Troyano**: Un *malware* que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

[19] **Cross-site scripting (XSS)** es un tipo de vulnerabilidad informática o agujero de seguridad típico de las aplicaciones Web, que puede permitir a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar (ej.: VBScript), se puede evitar usando medidas como CSP Política del mismo origen.
Es posible encontrar una vulnerabilidad de *Cross-Site Scripting* en aplicaciones que tengan entre sus funciones presentar la información en un navegador web u otro contenedor de páginas web. Sin embargo, no se limita a sitios web disponibles en Internet, ya que puede haber aplicaciones locales vulnerables a *XSS*, o incluso el navegador en sí.
XSS es un vector de ataque que puede ser utilizado para robar información delicada, secuestrar sesiones de usuario, y comprometer el navegador, subyugando la integridad del sistema. Las vulnerabilidades *XSS* han existido desde los primeros días de la Web.
Esta situación es usualmente causada al no validar correctamente los datos de entrada que son usados en cierta aplicación, o no sanear la salida adecuadamente para su presentación como página web.

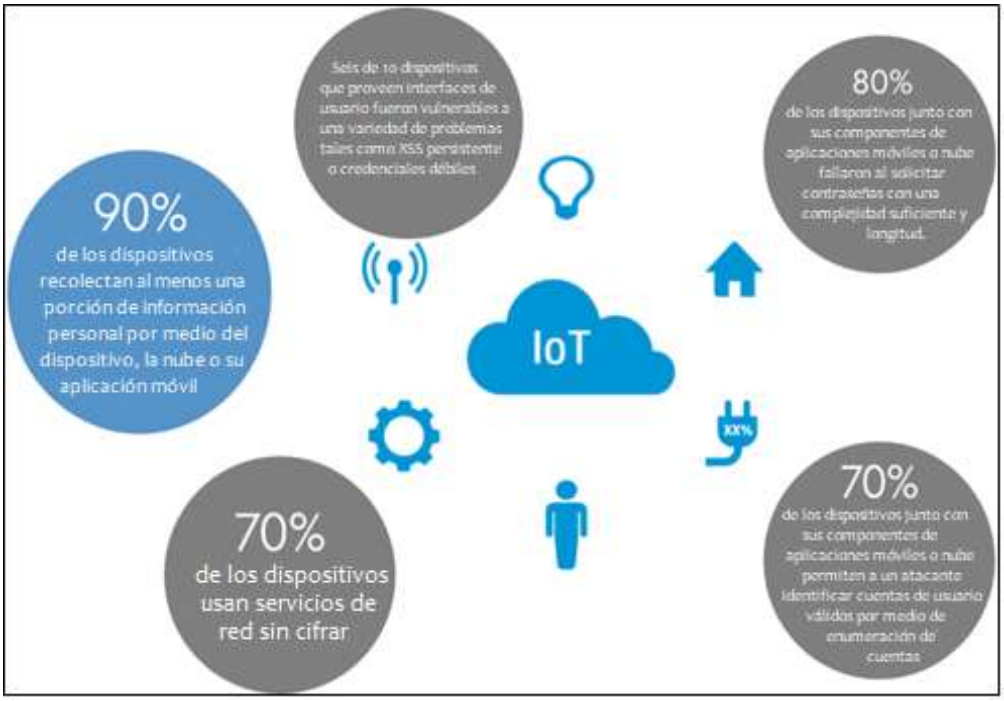


Ilustración 5 - Informe Vulnerabilidades HP en IoT de 2014
Fuente: https://i0.wp.com/onedigital.mx/ww3/wp-content/uploads/2014/08/HP-iot.jpg?resize=550%2C372

Especialistas como Vinton Cerf[20] (considerado como uno de los "padres" de internet) menciona como requisito prioritario la confidencialidad y la seguridad de la información en el ámbito de la conexión automática de dispositivos (Infobae, 2015).

Puede deducirse de los escenarios presentados en la introducción, que en el *IoT* existen tanto requerimientos como retos de seguridad que deben ser atendidos.

A continuación, se enumeran un resumen de éstos.

Requerimientos de seguridad

Según distintos investigadores, como Hossain e Islam que analizaron *IoT* asociados al cuidado de la salud, los requerimientos de seguridad de la *IoT* son similares a los

[20] **Vinton Gray Cerf** (New Haven, Connecticut, Estados Unidos, 23 de junio de 1943) es un científico de la computación estadounidense, considerado uno de los 'padres' de Internet. Se graduó en matemáticas y ciencias de la computación en la Universidad de Stanford (1965). Durante su estancia posterior en la Universidad de California (UCLA) obtuvo la maestría en ciencias y el doctorado. A principios de los años 70 comenzó a desarrollar con Robert Kahn un conjunto de protocolos de comunicaciones para la red militar, financiado por la agencia gubernamental DARPA. El objetivo era crear una "red de redes" que permitiera interconectar las distintas redes del Departamento de Defensa de los Estados Unidos, todas ellas de diferentes tipos y que funcionaban con diversos sistemas operativos, con independencia del tipo de conexión: radioenlaces, satélites y líneas telefónicas. Las investigaciones, lideradas por Vinton Cerf, primero desde la Universidad de California (1967-1972) y posteriormente desde la Universidad de Stanford (1972-1976), llevaron al diseño del conjunto de protocolos que hoy son conocidos como TCP/IP (*Transmission Control Protocol/Internet Protocol*), que fue presentado por Vinton Cerf y Robert Kahn en 1972

requerimientos de los sistemas de comunicación y procesamiento de información que conocemos como "tradicionales". (Islam, 2015)

1) **Disponibilidad**. Este principio es el encargado de garantizar la supervivencia de los servicios del *IoT* a usuarios autorizados (objetos o personas – Ver Confidencialidad) cuando sea necesario a pesar de los ataques a dichos servicios. Además, garantiza la entrega de un nivel mínimo de servicios ante la presencia de una pérdida de energía y/o falla.

2) **Confidencialidad**. Debe garantizar la inaccesibilidad de la información para usuarios y otros objetos, no autorizados. Adicionalmente, un mensaje confidencial debe resistir revelar su contenido a cualquier intruso.

3) **Integridad**. Persigue el principio que cualquier dato recibido no ha sido alterado o modificado en tránsito por algún adversario.

   Éste podría modificar la información y poner en peligro la integridad de la información en la *IoT*. Tampoco, la integridad de la información almacenada y su contenido deberían de ser comprometidos.

4) **No-repudiación**. Un nodo u objeto en el *IoT* no deberían poder negar el envío de un mensaje que ha enviado previamente.

5) **Autenticación**. Permite a un elemento que conforma la *IoT* garantizar la identidad de otros objetos con los que se comunica (por ejemplo, un receptor comprueba si los datos que ha recibido procedían de la fuente correcta o no). La autenticación es también necesaria para asegurar que únicamente usuarios válidos obtengan acceso para llevar a cabo las tareas administrativas sobre los dispositivos y redes del *IoT:* control remoto y/o reprogramación de los dispositivos y redes del *IoT*.

6) **Actualidad de la información**. Garantizar que los datos son recientes y no "repeticiones" de mensajes anteriores, es decir que sean "actuales".

7) **Autorización**. Es asegurar que sólo los dispositivos y los usuarios autorizados puedan obtener acceso a los servicios de red o a los recursos del *IoT*.

8) **Control de acceso**. Es el acto de asegurar que un nodo del *IoT* que ha sido autenticado tenga acceso solamente a lo que tiene autorizado y a nada más.

9) **Resiliencia**[21]. Es la garantía de que a pesar de que algunos dispositivos del *IoT* estén comprometidos, un esquema de seguridad debe continuar protegido contra ataques.

10) **Anonimato**. El anonimato oculta el origen de los datos. Este servicio de seguridad ayuda a la confidencialidad y la privacidad de los datos.

Retos de seguridad

Los requerimientos de seguridad en la *IoT* no pueden ser atendidos por las técnicas de seguridad tradicionales. La *IoT* impone nuevos retos para el desarrollo de técnicas novedosas que atiendan estos retos, entre los que se encuentran:

1) **Capacidad de cómputo limitada**. Los objetos y dispositivos de la *IoT* generalmente tienen procesadores embebidos que no son muy potentes en términos de su velocidad. Además, estos dispositivos no están diseñados para realizar operaciones costosas computacionalmente hablando. Es decir, que simplemente actúan como un sensor[22] o actuador[23]. Por lo tanto, encontrar una solución de seguridad que reduzca al mínimo el consumo de recursos y, por lo tanto, maximice la seguridad no es una tarea trivial.

2) **Memoria disponible limitada**. En comparación con un sistema tradicional digital (por ejemplo: PC, laptop, etc.), los objetos y dispositivos de la *IoT* están construidos con memoria *RAM* [24]y Flash limitada. Usan sistema operativo en tiempo real (*RTOS*)[25] o alguna versión ligera de un sistema operativo de propósito general (*GPOS*)[26], por ejemplo, Linux. También pueden ejecutar software de sistema y servicios propietarios.

[21] **Resiliencia**: Proceso de adaptarse bien a la adversidad, amenaza o fuentes de tensión significativas.

[22] **Sensor** es todo aquello que tiene una propiedad sensible a una magnitud del medio, y al variar esta magnitud también varia con cierta intensidad la propiedad, es decir, manifiesta la presencia de dicha magnitud, y también su medida.

[23] **Actuador** dispositivo capaz de transformar energía hidráulica, neumática o eléctrica en la activación de un proceso con la finalidad de generar un efecto sobre un proceso automatizado. Este recibe la orden de un regulador o controlador y en función a ella genera la orden para activar un elemento final de control, como por ejemplo una válvula. Son los elementos que influyen directamente en la señal de salida del automatismo, modificando su magnitud según las instrucciones que reciben de la unidad de control

[24] **Memoria RAM**: La memoria de acceso aleatorio (*Random Access Memory, RAM*) se utiliza como memoria de trabajo de computadoras y otros dispositivos para el sistema operativo, los programas y la mayor parte del software. En la *RAM* se cargan todas las instrucciones que ejecuta la unidad central de procesamiento (procesador) y otras unidades del computador, además de contener los datos que manipulan los distintos programas. Se denominan «de acceso aleatorio» porque se puede leer o escribir en una posición de memoria con un tiempo de espera igual para cualquier posición, no siendo necesario seguir un orden para acceder (acceso secuencial) a la información de la manera más rápida posible. Es una memoria volátil. Si se apaga el equipo, se pierden los datos allí almacenados.

[25] **RTOS**: *Real Time Operating System*. Sistema Operativo de Tiempo Real.

[26] **GPOS**: *General Purpose Operating System*. Sistema Operativo de Propósitos Generales.

Por lo tanto, los sistemas de seguridad deben ser eficientes en el uso de memoria. Sin embargo, los algoritmos de seguridad tradicionales no se diseñaron específicamente para ser eficientes en el uso de ésta, ya que los sistemas digitales tradicionales utilizan una gran cantidad de memoria *RAM* en asociación a un disco rígido de alta capacidad de almacenamiento. Por lo tanto, los algoritmos de seguridad convencionales no pueden utilizarse directamente en los dispositivos de la *IoT*.

3) **Energía disponible limitada**. Un objeto inteligente en la *IoT* generalmente incluye una batería como medio de suministro de energía para los sensores y los actuadores de abordo (por ejemplo, sensor de temperatura, acelerómetro, *GPS*[27], etc.). Los objetos inteligentes administran el uso de energía mediante la activación del modo de ahorro de energía cuando no hay una lectura del sensor que deba ser informada.

Adicionalmente, el procesador de abordo funciona a baja velocidad si no hay nada importante que se vaya a procesar. Por lo tanto, la restricción energética, propia de los objetos inteligentes en la *IoT*, hace que sea difícil encontrar una solución de seguridad que minimice el uso de energía.

4) **Movilidad**. La movilidad es uno de los principales atributos de los objetos y dispositivos en la *IoT*, donde los dispositivos se pueden conectar a una red local próxima sin configuración previa. Esta característica de movilidad plantea la necesidad de desarrollar algoritmos de seguridad que se adapten a está movilidad de los objetos y dispositivos en esta tecnología.

5) **Escalabilidad**. Como fuera enunciado anteriormente, el número dispositivos en la *IoT* está creciendo día a día y más dispositivos se conectan a la red mundial de información, Internet.

Los sistemas de seguridad actuales no están diseñados con la propiedad de escalabilidad, por lo tanto, no son adecuados para aplicarse en los dispositivos de la *IoT*.

6) **Multitud de estándares de comunicación**. En general, los dispositivos están conectados a las redes locales y globales a través de una amplia gama de enlaces

[27] **GPS**: El Sistema de Posicionamiento Global (en inglés, *GPS*; *Global Positioning System*) es un sistema que permite determinar en toda la Tierra la posición de cualquier objeto (una persona, un vehículo) con una precisión de hasta centímetros (si se utiliza *GPS* diferencial), aunque lo habitual son unos pocos metros de precisión. Para determinar su posición, un usuario utiliza 4 o más satélites y utiliza la trilateración.

inalámbricos basados en protocolos como Zigbee (explicado en profundidad más adelante), *Z-Wave*[28], *Bluetooth*[29], *Bluetooth* de bajo consumo de energía[30], *WiFi*[31], *GSM*[32], *WiMax*[33] y *3G*[34]/*4G*[35], entre otros. Las características del canal de comunicación inalámbrico de estas redes hacen que los esquemas de seguridad diseñados para canales de comunicación con redes cableadas sean inapropiados. Por lo tanto, es difícil diseñar protocolos de seguridad que sean aplicables tanto en redes cableadas como en redes inalámbricas por igual.

7) **Multiplicidad de dispositivos**. Los dispositivos en la *IoT* son muy diversos, van desde las computadoras personales (*PCs*) totalmente equipadas hasta la gama baja de etiquetas de identificación por radiofrecuencia (*RFID*)[36]. Este tipo de dispositivos varían en términos de su capacidad de su cómputo, potencia de alimentación, memoria y el software incorporado. Por lo tanto, el reto consiste en diseñar un esquema de seguridad que puede albergarse incluso en el más sencillo de estos objetos o dispositivos de la *IoT*.

[28] **Z-Wave**: Protocolo de comunicaciones inalámbricas utilizado principalmente para domótica. Es una red en malla que utiliza ondas de radio de baja energía para comunicarse de un aparato a otro, permitiendo el control inalámbrico de electrodomésticos y otros dispositivos, como control de iluminación, sistemas de seguridad, termostatos, ventanas, cerraduras, piscinas y garaje con puertas automatizadas.

[29] **Bluetooth**: Especificación industrial para Redes Inalámbricas de Área Personal (*WPAN*) creado por *Bluetooth Special Interest Group, Inc*. que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2.4 GHz

[30] **Bluetooth Low Energy**: (Bluetooth LE, coloquialmente BLE) es una tecnología de red de área personal inalámbrica. Destinada a aplicaciones novedosas en el cuidado de la salud, fitness y *beacons*, seguridad y las industrias de entretenimiento en el hogar. Comparado con el *Bluetooth* clásico, *Bluetooth Low Energy* está diseñado para proporcionar un bajo consumo de energía y a costos considerablemente reducidos, manteniendo un rango de alcance de comunicación similar.

[31] **Wifi:** (escrito también wi fi) es una tecnología que permite la interconexión inalámbrica de dispositivos electrónicos. Los dispositivos habilitados con wifi (tales como computadoras personales, teléfonos, televisores, etc.) pueden conectarse entre sí o a internet a través de un punto de acceso de red inalámbrica. Cumplen con los estándares 802.11 relacionados con redes inalámbricas de área local.

[32] **GSM**: El sistema global para las comunicaciones móviles (del inglés *Global System for Mobile communications*) es un sistema estándar, libre de regalías, de telefonía móvil digital.

[33] **WiMax**: Siglas de *Worldwide Interoperability for Microwave Access* (interoperabilidad mundial para acceso por microondas), es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2,5 a 5,8 GHz y puede tener una cobertura hasta de 70 km. Es una tecnología dentro de las conocidas como tecnologías de última milla, también conocidas como bucle local que permite la recepción de datos por microondas y retransmisión por ondas de radio. El estándar que define esta tecnología es el IEEE 802.16

[34] **3G**: Abreviación de Tercera Generación de transmisión de voz y datos a través de telefonía móvil mediante UMTS (*Universal Mobile Telecommunications System* o servicio universal de telecomunicaciones móviles). Los servicios asociados con la tercera generación proporcionan la posibilidad de transferir voz y datos no-voz (como la descarga de programas, intercambio de correos electrónicos, y mensajería instantánea).

[35] **4G**: En telecomunicaciones, 4G es la sigla utilizada para referirse a la cuarta generación de tecnologías de telefonía móvil. La 4G está basada completamente en el protocolo IP, siendo un sistema y una red, que se alcanza gracias a la convergencia entre las redes de cable e inalámbricas. Esta tecnología podrá ser usada por módems inalámbricos, móviles inteligentes y otros dispositivos móviles.

[36] **RFID** o **identificación por radiofrecuencia** (del inglés *Radio Frequency Identification*) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, tarjetas o transpondores RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio

8) **Topología dinámica de red**. Los objetos y dispositivos en la *IoT* pueden unirse o abandonar una red en cualquier momento desde cualquier lugar. Esta característica de los objetos y dispositivos, de dinámicamente conectarse y desconectarse tanto temporal como espacialmente, requiere la existencia de una topología dinámica de red. Los esquemas de seguridad existentes para los sistemas digitales tradicionales no consideran este tipo de red en donde pueden existir cambios repentinos de topología. Por lo tanto, un modelo de seguridad tradicional no es directamente aplicable en los objetos y dispositivos inteligentes de la *IoT*.

9) **Red Multiprotocolo**. Los objetos y dispositivos del *IoT* podrían utilizar un protocolo de red propietario (por ejemplo, diferente al protocolo *IP*) para la comunicación con redes locales. Al mismo tiempo, podrían comunicarse con un proveedor de servicios a través de redes *IP*. Estas características hacen que los protocolos de comunicación tradicionales no sean adecuados para sistemas de seguridad en dispositivos de la *IoT*.

10) **Actualización dinámica de protocolos de seguridad**. Para mitigar las vulnerabilidades potenciales, es necesario seguir protocolos de seguridad actualizados al día. Por lo tanto, las actualizaciones continuas de los protocolos de seguridad en los dispositivos de la *IoT* son necesarias. Sin embargo, diseñar un mecanismo dinámico para la instalación de parches de seguridad es una tarea difícil.

11) **Encapsulado de sensores y dispositivos a prueba de ser manipulados o abiertos**. Una característica que generalmente no considerada de manera apropiada es la seguridad física de los objetos y dispositivos de la *IoT*. Un atacante podría manipular físicamente los dispositivos y tal vez podría extraer secretos criptográficos, modificar los programas residentes en el dispositivo, o sustituir a los nodos con nodos maliciosos.

Un embalaje resistente a las manipulaciones y a la apertura es una forma de defenderse de estos ataques, pero el diseño y construcción de este tipo de embalaje es difícil de realizar en la práctica, tanto por su diseño como por su costo.

Vulnerabilidades de Seguridad

Taxonomía de ataques

Un atacante podría fraguar diferentes tipos de amenazas a la seguridad y comprometer los dispositivos y objetos de la *IoT*. Algunas amenazas son tangibles, algunas son predecibles, y muchas son difíciles de predecir. Las amenazas existentes en este ámbito pueden clasificarse basándose en tres propiedades principales:

- ataques a la información,
- ataques basados en las propiedades del objeto o dispositivo y
- ataques basados en las propiedades de la red.

1) **Ataques a la información**. La información que se encuentra en tránsito podría ser manipulada o analizada por un atacante con el fin de alterar dicha información o eliminarla. Entre este tipo de ataques se encuentran:

a) **Interrupción de servicio**. Un adversario realiza un ataque de denegación de servicio con el fin de causar que el enlace de comunicación se vea interrumpido o no disponible.

b) **Intercepción:** Es cuando un adversario captura (escucha) la información en tránsito amenazando la privacidad y confidencialidad de la información.

c) **Modificación:** Un adversario que obtiene acceso no autorizado a la información puede alterarla o modificarla con el fin de crear confusión y engañar a los usuarios.

d) **Fabricación:** En este caso el adversario cambia mensajes inyectando información falsa amenazando la autenticidad de la información y confundir a los usuarios.

e) **Reenvío:** En este caso un adversario reenvía información existente amenazando la actualidad (*freshness*) de la información creando confusión y engañando a los usuarios.

2) **Ataques basados en las propiedades del objeto o dispositivo de la *IoT***. Esta clasificación está compuesta por tres tipos de ataques:

a) **Usuario comprometido:** Un adversario compromete los dispositivos y red del usuario siendo atacado por engaño o robo; este ataque puede revelar información sensitiva como claves de acceso, llaves de cifrado y datos sensibles del usuario.

b) **Hardware comprometido:** Un adversario manipula físicamente el hardware del objeto o dispositivo con el fin de extraer el código a bordo del dispositivo, las llaves de cifrado o la información almacenada; también un atacante podría reprogramar el dispositivo comprometido con código malicioso.

c) **Software comprometido:** En este caso el atacante explota las vulnerabilidades del software, por ejemplo, el sistema operativo, el *firmware*[37] y las aplicaciones, con el fin de provocar un malfuncionamiento o forzar algún estado disfuncional del dispositivo (por ejemplo, desbordamiento de memoria y agotamiento de recursos).

3) **Ataques basados en las propiedades de la red**. En esta categoría son descriptas dos formas de ataque:

a) **Protocolo estándar comprometido**: Un atacante utiliza los protocolos estándar para actuar de manera maliciosa con el fin de amenazar la disponibilidad, privacidad, integridad y autenticidad de la información.

b) **Ataque a la pila del protocolo de red**: Considerando la pila de protocolo de red para la *IoT* propuesta por la *Internet Engineering Task Force* (*IETF*)[38], ésta tiene diferentes tipos de vulnerabilidades en cada capa que un adversario podría explotar para realizar actividades maliciosas.

[37] **Firmware**: El *firmware* o soporte lógico inalterable es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Está fuertemente integrado con la electrónica del dispositivo, es el software que tiene directa interacción con el hardware, siendo así el encargado de controlarlo para ejecutar correctamente las instrucciones externas. En resumen, un *firmware* es un software que maneja físicamente al hardware.

[38] **Internet Engineering Task Force (IETF):** Organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Se creó en los Estados Unidos, en 1986. Es mundialmente conocido porque se trata de la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC.
Es una institución sin fines de lucro y abierta a la participación de cualquier persona, cuyo objetivo es velar para que la arquitectura de Internet y los protocolos que la conforman funcionen correctamente. Se la considera como la organización con más autoridad para establecer modificaciones de los parámetros técnicos bajo los que funciona la red. El IETF se compone de técnicos y profesionales en el área de redes, tales como investigadores, integradores, diseñadores de red, administradores, vendedores, entre otros.

2. Limitaciones y alcances del trabajo

En el proceso de investigación se incluyó la búsqueda de *papers*, otras tesis, apuntes de materias de grado, material periodístico, material de blogs y sitios especializados, informes de fabricantes y búsquedas por internet para obtener el estado del arte de la tecnología de *IoT*, los usos de ésta y de los riesgos asociados para avanzar en la investigación.

Se analizaron distintos protocolos utilizados para la interrelación de los dispositivos y los métodos de autenticación utilizados por éstos.

3. Hipótesis de trabajo

Es posible realizar una estandarización de los requerimientos y/o elementos a tener en cuenta para asegurar la autenticación en el uso de Internet de las Cosas, incluyendo todos los participantes "humanos" de la nueva arquitectura: Consumidores, Desarrolladores, Fabricantes y Testers de manera de reducir la exposición a los riegos asociados a una autenticación débil o inexistente.

4. Objetivos

El presente trabajo persigue los siguientes objetivos:

Objetivo de Investigación:

Lograr una mejora en el proceso de autenticación en las implementaciones de Internet de las Cosas

Objetivos Específicos:

- Identificar los requerimientos y las limitaciones de la tecnología *IoT*.
- Identificar los riesgos asociados a dicha tecnología.
- Identificar los ámbitos de aplicación.
- Identificar las falencias de los distintos procesos de autenticación en las implementaciones más utilizadas.
- Identificar los protocolos de comunicación/administración más utilizados.
- Analizar las buenas prácticas de la industria para el aseguramiento relacionados a IoT.
- Analizar la creación de estándares de aseguramiento

5. Lineamientos Metodológicos

Como lineamientos metodológicos, se ha decidido adoptar las siguientes alternativas de investigación:

- Estudio y Análisis del estado del arte.
- Estudio y Análisis de problemas y vulnerabilidades relacionados con la *IoT*
- Estudio y Análisis de implementaciones sobre los protocolos más utilizados
- Estudio y Análisis de diferentes metodologías de autenticación en uso en el ámbito de *IoT* y estudio de compatibilidades para la implementación de la autenticación fuerte.
- Estudio y Análisis de Mejores Prácticas / Recomendaciones de Organizaciones relacionadas a la seguridad

6. Estructura General del Trabajo

El presente trabajo, contiene una introducción al tema en el cual se encuentra inmerso describiendo tanto su entorno actual como futuro.

Para una mejor organización se encuentra divido en 7 capítulos, cada uno con los apartados correspondientes.

Capítulo I: Contexto de la Investigación

En esta sección son introducidos los conceptos que describen el contexto actual en la cual se encuentra inmersa *IoT*.

Se realiza un análisis respecto al mercado actual y futuro respecto a las implementaciones.

También se plantean distintos ejemplos sobre fallas en la seguridad de esta tecnología, de manera de situarnos en la problemática a la cual nos enfrentaremos masivamente, en un futuro no muy lejano, si no se realizan las acciones pertinentes al aseguramiento.

Capítulo II: Marco de Estudio

En este capítulo son evidenciadas distintas implementaciones. Serán analizados los 2 protocolos más utilizados y las vulnerabilidades asociadas a la tecnología propiamente dicha y a las estrategias utilizadas en la implementación.

Permite conocer también el "estado del arte" respecto a Internet de las Cosas, describiendo algunos de los posibles usos, con sus respectivas ventajas, y algunos problemas encontrados en las distintas instalaciones.

Capítulo III: De la situación problemática a la solución

Conociendo el problema descripto, se analizarán las distintas opciones actuales para atacarlos.

Las medidas analizadas, muchas veces, terminan siendo paliativas o forenses, dependiendo del momento en el cual se las tome en cuenta.

Una práctica recomendada sería tomar los distintos esfuerzos, que ya han realizado otras instituciones y organismos, para no volver a cometer los mismos errores una y otra vez. Errores que pertenecieron a otros tiempos y otras tecnologías, y que ya se encontraban superados, pero que, por estas nuevas maneras de interconectar la gran variedad de equipos, vuelven a recobrar impulso.

Capítulo IV: Solución

Como una solución, más cercana a lo definitivo, se plantea la organización de estándares, con la participación de todos los niveles de este ecosistema

- Gobierno,
- Fabricantes
- Instituciones Educativas
- Comunidades y Organizaciones sin fines de lucro relacionadas con el tema
- Usuarios finales.

Incluyendo también la utilización de las buenas prácticas, verificaciones y análisis contra propuestas de organizaciones que trabajan para asegurar o que, al menos, sepamos qué tan inseguros podemos estar, con el uso de esta tecnología.

Teniendo en cuenta todas estas variables, podría generarse un estado de seguridad desde el propio diseño de los dispositivos, asegurar que cumplan con regulaciones que establezcan los valores mínimos a cumplir y que despejen dudas a todos los participantes.

Capítulo V: Validación

Este apartado presenta un desafío importante, porque hay que analizar si todos los participantes del ecosistema están dispuestos a comenzar a crear un camino para asegurar la tecnología que generará, sin duda alguna, una revolución en la manera de gestionar los dispositivos, la información que ellos generen, en los distintos lugares donde se las implemente.

Se realizaron búsquedas sobre trabajos realizados, ya no como meras investigaciones, sino qué, pertenecientes al mundo real.

Capítulo VI: Conclusiones y futuros trabajos

Aquí puede evidenciarse que se está yendo por el camino correcto. Aunque, posiblemente, no en la secuencia o velocidad de implementación deseada.

Hubiera sido deseable realizar algunos pasos previos antes de "sacar a la calle" semejante revolución tecnológica. (concepto planteado anteriormente).

También se propondrán los distintos trabajos futuros.

Capítulo VII: Bibliografía

En este apartado serán detalladas las fuentes consultadas y citadas en el trabajo.

(Página en blanco)

CAPITULO II – Marco de Estudio

(Página en blanco)

Internet de las Cosas (*IoT*, siglas en inglés de "*Internet of Things*")

1. Definición

El concepto de la "Internet de las Cosas" no es nuevo: el término fue acuñado por el pionero tecnológico británico Kevin Ashton en 1999 en el *MIT*. (Ashton, 2009)

Consiste en la interconexión de objetos físicos a Internet, independientemente de su ubicación, los cuales intercambian datos – ya sea generando o consumiendo la información ya generada – con un usuario, con terceros o con otros dispositivos.

En caso de que las "cosas" como, termostatos, heladeras, paquetes, lámparas, botiquines, partes automotrices, etc. estuvieran conectados a Internet y equipados con dispositivos de identificación no existirían, en teoría, cosas fuera de stock o carencia y/o caducidad de medicinas, sabríamos exactamente la ubicación, cómo se consumen y se compran productos en todo el mundo. El extravío sería cosa del pasado y podría saberse qué está encendido o apagado en todo momento.

2. Tipos de Uso

Hogareño

En el entorno hogareño cada vez más electrodomésticos se suman a *IoT*: lavarropas, heladeras, hornos, aspiradoras, aires acondicionados permitiendo ser monitoreados y controlados remotamente. De la misma manera, se suman monitoreo cámaras, alarmas domiciliarias, sensores de escapes de gas, encendido remoto de luces, botones de pánico, medidores de consumo de servicios públicos y la lista se va incrementando todos los días.

Ilustración 6 - Hogar y dispositivos IoT
Fuente: https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones

Existe una multiplicidad de fabricantes y protocolos que participan en esta categoría.

Dicha situación aumenta la complejidad y heterogeneidad del ecosistema. (INCIBE, 2019)

Muchos dispositivos de este entorno utilizan el protocolo ZigBee (que será descripto en profundidad más adelante).

Uso Industrial

Ante la aparición de estos dispositivos, comenzó a gestarse el concepto de "Industria 4.0" o "Cuarta Revolución Industrial", representada en la "ilustración 7", que podría ser definida como la como la digitalización completa a través de la integración de tecnologías de procesamiento de datos, software inteligente y sensores, desde los proveedores hasta los clientes.

Pero para que esta idea pueda ser llevada a cabo, los dispositivos deben poder comunicarse, tanto entre sí, como hacía el exterior. Algo que, a partir de *IoT* sería posible.

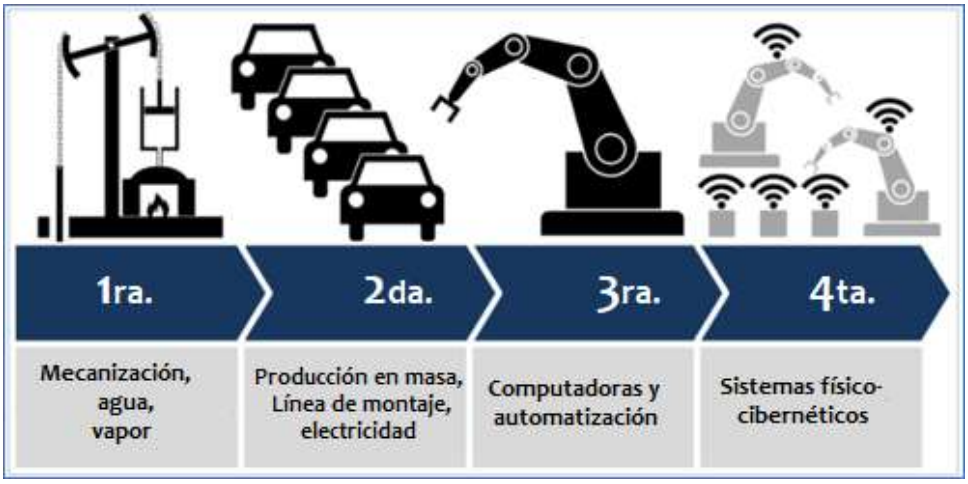


Ilustración 7 - Revoluciones Industriales
Fuente: https://es.wikipedia.org/wiki/Revoluci%C3%B3n_industrial_etapa_cuatro#/media/Archivo:Industry_4.0.png

La interconexión de los sistemas para tomar datos de sensores, tomar acciones con actuadores, generar información para control de stock, pedidos o programación de la producción de manera automatizada y todo otro tipo de operaciones son parte del concepto "Industria 4.0", representado en la siguiente ilustración:

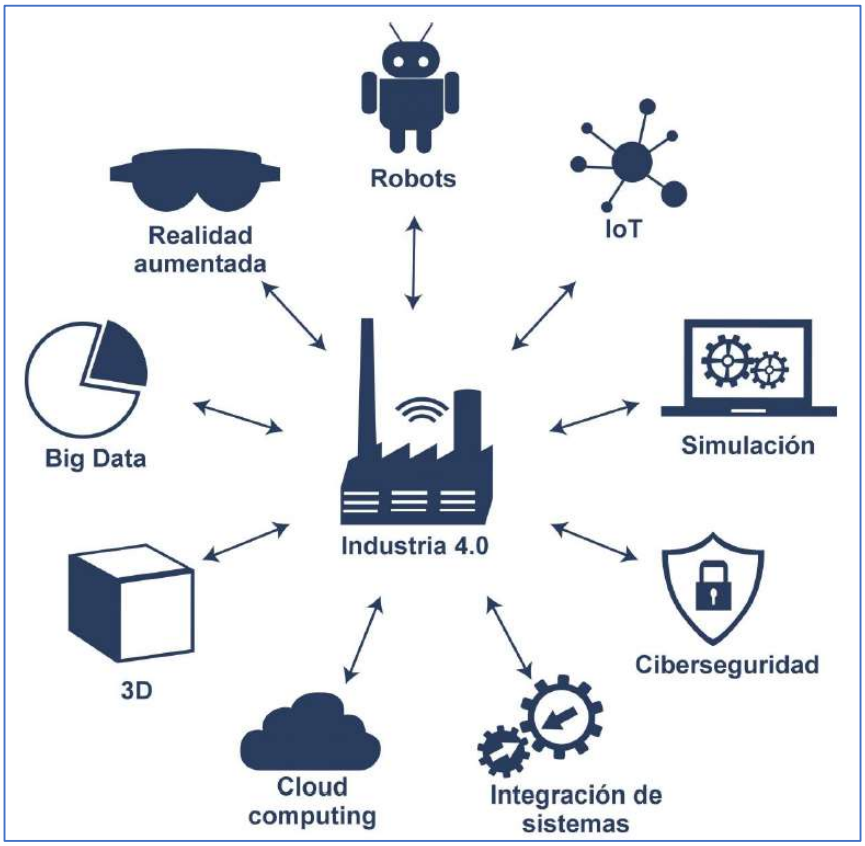


Ilustración 8 - Visión Industria 4.0
Fuente: https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones

En este entorno, hay una multiplicidad de protocolos que actúan:

- **MQTT** *(Message Queuing Telemetry Transport)*

Es un protocolo de tipo publicación/suscripción de nivel de aplicación. Este protocolo ha sido implementado en múltiples aplicaciones de *IT* y de *IoT*.

Se encuentran implementaciones de este protocolo en:

  - Messenger de Facebook,
  - MS Azure IoT hub
  - Amazon AWS
  - IBM

- **AMQP** (*Advanced Message Queuing Protocol*)

Es un protocolo del nivel 7 del modelo OSI[39] para aplicaciones distribuidas que soporta comunicaciones punto-a-punto y de tipo publicación/suscripción. Proviene del sector de servicios financieros y tiene presencia en el ámbito de TI y en el sector industria, siendo bastante limitada en este último.

- **CoAP** *(Constrained Application Protocol)*

Fue creado por *IETF* para proveer la compatibilidad de *HTTP*[40] con una mínima carga. Es un protocolo cliente/servidor, es similar a *HTTP,* pero usa *UDP*[41]/multicast en lugar de *TCP*[42], además de simplificar el encabezado reduce el tamaño de cada requerimiento. Desde el punto de vista de la seguridad utiliza *DTLS*[43]*,* que básicamente consiste en aplicar seguridad en la capa de transporte para proteger las comunicaciones.

[39] "**Modelo OSI**", (en inglés, *Open System Interconnection*) El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1). Es un modelo de referencia para los protocolos de la red (no es una arquitectura de red), creado en el año 1980 por la Organización Internacional de Normalización (ISO). Se ha publicado desde 1983 por la Unión Internacional de Telecomunicaciones (UIT)

[40] **HTTP** (*HyperText Transfer Protocol*, Protocolo de transferencia de hipertexto) Permitir la transferencia de archivos (principalmente, en formato *HTML*). entre un navegador (el cliente) y un servidor web localizado mediante una cadena de caracteres denominada dirección URL.

[41] **UDP**: El protocolo de datagramas de usuario (en inglés: *User Datagram Protocol*) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 o de Transporte del Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción.

[42] **TCP**: Protocolo de control de transmisión (en inglés *Transmission Control Protocol*) es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

[43] **DTLS**: *Datagram Transport Layer Security* es un protocolo que proporciona privacidad en las comunicaciones para protocolos de datagramas. Este protocolo permite a las aplicaciones cliente/servidor comunicarse de manera que se eviten las escuchas no deseadas (*eavesdropping*), accesos no permitidos, o modificación de mensajes. El protocolo DTLS está basado en el protocolo TLS y proporciona garantías de seguridad equivalentes

- **HTTP (REST[44]/JSON[45]) (Hypertext Transfer Protocol)**

Es un protocolo cliente/servidor sin conexión presente en las TIC y en la web. Es un protocolo muy accesible por ser de código abierto, además de poseer numerosas librerías. Es efectivo para enviar grandes cantidades de información, como por ejemplo lecturas de sensores minuto a minuto o cada hora; aunque no es adecuado ni para enviar actualizaciones en periodos de tiempo del orden de milisegundos ni para enviar información de video. Es muy recomendable asegurar la información transmitida aplicando el protocolo criptográfico *SSL*[46]/*TLS*[47] sobre *HTTP*, lo que genera el protocolo de aplicación *HTTPS*[48].

No obstante, el método más seguro consiste en incluir en el dispositivo *IoT* solo un cliente *HTTP*, no un servidor *HTTP*, de manera que el dispositivo *IoT* pueda iniciar conexiones a un servidor web, pero no sea capaz de recibir solicitudes de conexión.

Smart Cities

Una *Smart City* (en castellano "Ciudad Inteligente") es aquella ciudad que usa las tecnologías de la información y las comunicaciones para hacer que tanto su infraestructura crítica, como sus componentes y servicios públicos ofrecidos sean más interactivos, eficientes y los ciudadanos puedan ser más conscientes de ellos (Fundación Telefónica, 2011). Combinando los espacios digitales y físicos en un ecosistema complejo con importante cantidad de sensores e información a recolectar, transmitir y procesar.

[44] **REST** deriva de "*REpresentational State Transfer*". La clave de REST es que un servicio REST no tiene estado (es stateless), lo que quiere decir que, entre dos llamadas cualesquiera, el servicio pierde todos sus datos. Esto es, que no se puede llamar a un servicio REST y pasarle unos datos (p. ej. un usuario y una contraseña) y esperar que "nos recuerde" en la siguiente petición. De ahí el nombre: el estado lo mantiene el cliente y por lo tanto es el cliente quien debe pasar el estado en cada llamada. Si quiero que un servicio REST me recuerde, debo pasarle quien soy en cada llamada. Eso puede ser un usuario y una contraseña, un token o cualquier otro tipo de credenciales, pero debo pasarlas en cada llamada. Y lo mismo aplica para el resto de información.

[45] **JSON** (acrónimo de *JavaScript Object Notation*, «notación de objeto de JavaScript») es un formato de texto sencillo para el intercambio de datos. Se trata de un subconjunto de la notación literal de objetos de JavaScript, aunque, debido a su amplia adopción como alternativa a XML, se considera (año 2019) un formato independiente del lenguaje.

[46] **SSL** es el acrónimo de *Secure Sockets Layer* (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal. Los dos sistemas pueden ser un servidor y un cliente (por ejemplo, un sitio web de compras y un navegador) o de servidor a servidor (por ejemplo, una aplicación con información que puede identificarse como personal o con datos de nóminas).

[47] **TLS**: del inglés Transport Layer Security (en español seguridad de la capa de transporte) es un protocolo criptográfico, que proporcionan comunicaciones seguras por una red, comúnmente Internet. Utiliza criptografía asimétrica para autentificar a la contraparte con quien se están comunicando y para intercambiar una llave simétrica.

[48] **HTTPS**: El Protocolo seguro de transferencia de hipertexto (en inglés: *Hypertext Transfer Protocol Secure* o *HTTPS*), es un protocolo de aplicación basado en el protocolo *HTTP*, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de *HTTP*. Utiliza un cifrado basado en la seguridad de textos *SSL/TLS* para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo *HTTP*. De este modo se consigue que la información sensible (usuario y claves de paso normalmente) no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar. El puerto estándar para este protocolo es el 443. (También comúnmente usado el 4433)

La participación de los dispositivos en el apartado de servicios está dada, por ejemplo, en:

- monitoreo por contaminación,
- botones de pánico en la vía pública,
- eficiencia de tráfico,
- estacionamiento inteligente,
- iluminación activa,
- administración de residuos, etc.

En la misma se plantean ahorros en provisión de servicios, consumo de energía e insumos, tiempos, entre otros. Tal como es representado en la siguiente ilustración:

Área de aplicación	Ahorro
Riego de parques y jardines	15% del agua utilizada
Recogida de basuras	25% en requerimiento de transporte según el tipo de residuos
Gestión del tráfico	17% de emisiones de CO_2 a la atmósfera
Smart Metering	10% en el consumo de energía eléctrica. 7% en el consumo de agua particular

Ilustración 9 - Ejemplo Ahorro Málaga Smart City 2011
Fuente: https://www.fundaciontelefonica.com/cultura-digital/publicaciones/101/

Otro ámbito de aplicación es la Infraestructura en las ciudades:

- alerta temprana de inundaciones,
- monitoreo de agua potable,
- estaciones meteorológicas,
- control de cadena de frío, trazabilidad de bienes,
- redes inteligentes de energía,
- aplicaciones de salud, etc.

En esta clasificación se encuentran incluías las interconexiones entre hogares y proveedores de servicios públicos (energía eléctrica, etc.) que tienden a usar medidores inteligentes. Este tipo de dispositivos suelen implementarse con tecnología ZigBee.

3. Componentes

Dentro de los componentes que conforman "IoT" pueden encontrarse

- Comunicación (*Wireless*[49], cableada, celular, infrarrojo, *RFID*, *Wifi*, *Bluetooth*.)
- Sensores (Video, audio, posicionamiento, acelerómetros, temperatura, proximidad, lectores *RFID*, etc.)
- Actuadores
- Almacenamiento (Bases de Datos, *DHT* - tablas de hash distribuidas[50], etc.)
- Dispositivos (actuadores, "cosas", laptops, sensores, teléfonos celulares, lectores y tags *RFID*, etc.)
- Procesamiento (Servicios, Redes de Sensores locales y globales, procesamiento in cloud, etc.)
- Localización y Seguimiento (*RFID*, *GSM*, *GPS*, Sensores, etc.)
- Identificación (códigos de barra, *RFID*, 2D Tags, Biometría, Video, etc.)

4. Protocolos más utilizados

Como hemos mencionado, los protocolos más utilizados son *MQTT* y ZigBee, sobre los cuales haré una descripción más profunda, analizando la manera en la cual trabajan.

Protocolo MQTT

MQTT (*Message Queue Telemetry Transport*) es un protocolo usado para la comunicación machine-to-machine (*M2M*)[51] en la "*Internet of Things*".
Está basado en un protocolo de mensajería creado por los ingenieros Dr. Andy Stanford-Clark de IBM y Arlen Nipper de Eurotech, en 1999 (Yuan, 2018).

[49] **Wireless**: palabra del idioma inglés que puede traducirse como "sin cables" o "inalámbrico". Su uso, por lo tanto, podría estar vinculado a cualquier tipo de comunicación que no requiere de un medio de propagación físico. Sin embargo, la noción de *wireless* se utiliza principalmente para nombrar a las comunicaciones inalámbricas en el marco de las tecnologías informáticas.
[50] **DHT** *Distributed Hash Table*: Una tabla hash distribuida es una clase de un sistema distribuido descentralizado que proporciona un servicio de búsqueda similar a una tabla hash: los pares (clave, valor) se almacenan en un *DHT*, y cualquier nodo participante puede recuperar de manera eficiente el valor asociado con una clave dada Las claves son identificadores únicos que se asignan a valores particulares, que a su vez pueden ser desde direcciones, documentos y datos arbitrarios. La responsabilidad de mantener la asignación de claves a valores se distribuye entre los nodos, de tal manera que un cambio en el conjunto de participantes cause una cantidad mínima de interrupción. Esto le permite a un *DHT* escalar a un número extremadamente grande de nodos y manejar las continuas llegadas, salidas y fallas de nodos.
[51] **M2M**: (*machine to machine*, 'máquina a máquina') es un concepto genérico que se refiere al intercambio de información o comunicación en formato de datos entre dos máquinas remotas.

Este protocolo está orientado a la comunicación de sensores, debido a que consume muy poco ancho de banda y puede ser utilizado en la mayoría de los dispositivos integrados, incrustados o embebidos con pocos recursos (*CPU*, *RAM*, …), tal como lo grafica la "ilustración 10".
Además de ser un estándar, es de código abierto. La especificación del protocolo se ha publicado abiertamente con una licencia libre. Fue en el año 2011 cuando las empresas IBM y Eurotech donaron el código *MQTT* al proyecto Eclipse[52]. A final de 2014, se convirtió oficialmente en un patrón abierto OASIS, con soporte en los lenguajes de programación populares, usando diversas implementaciones de software libre. (OASIS, 2014)

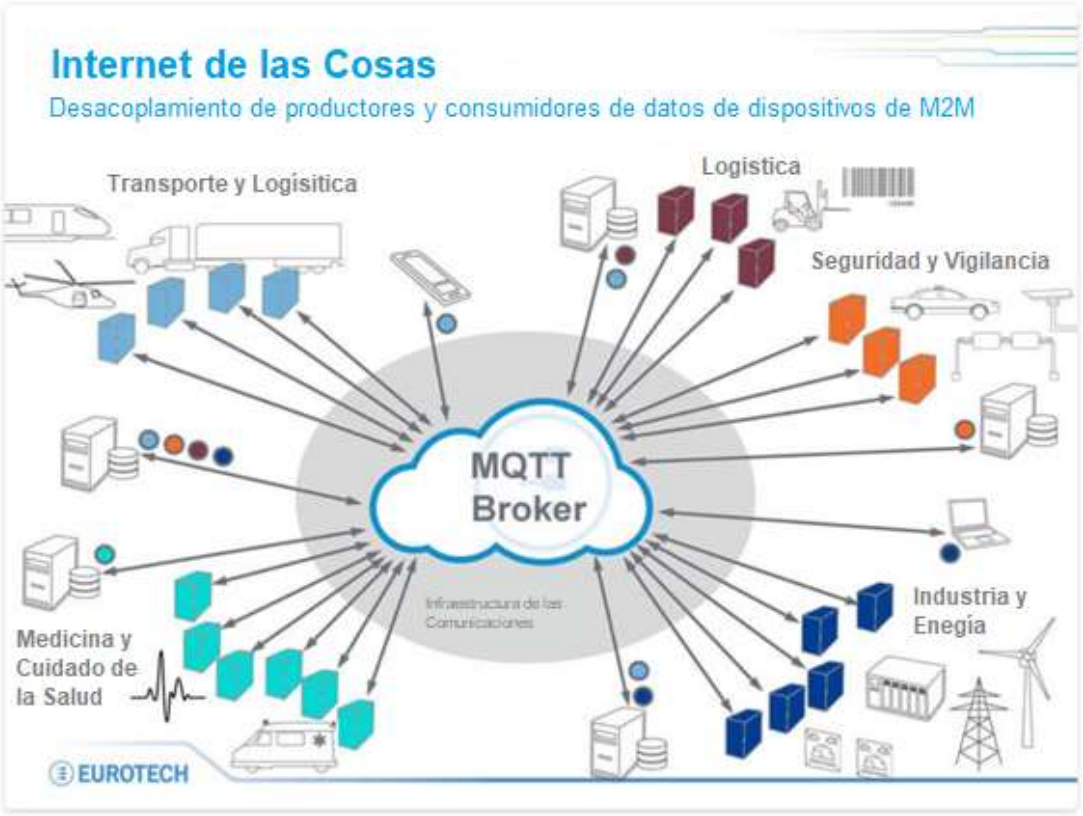


Ilustración 10 - Entorno del protocolo MQTT
Fuente: https://aprendiendoarduino.wordpress.com/2018/11/19/mqtt/

Arquitectura de un sistema MQTT

Todos los dispositivos "clientes" se conectan directamente a un punto central que hace de servidor, llamado "*Broker*", el cual es la parte central y todos los mensajes pasan por él, tal como lo grafica la "ilustración 11".

[52] **Eclipse** es una plataforma de software compuesto por un conjunto de herramientas de programación de código abierto multiplataforma para desarrollar lo que el proyecto llama "Aplicaciones de Cliente Enriquecido", opuesto a las aplicaciones "Cliente-liviano" basadas en navegadores. Esta plataforma, típicamente ha sido usada para desarrollar entornos de desarrollo integrados (del inglés IDE), como el IDE de Java llamado Java Development Toolkit (JDT) y el compilador (ECJ) que se entrega como parte de Eclipse (y que son usados también para desarrollar el mismo Eclipse).

Esa conexión está dada por medio de suscripciones.

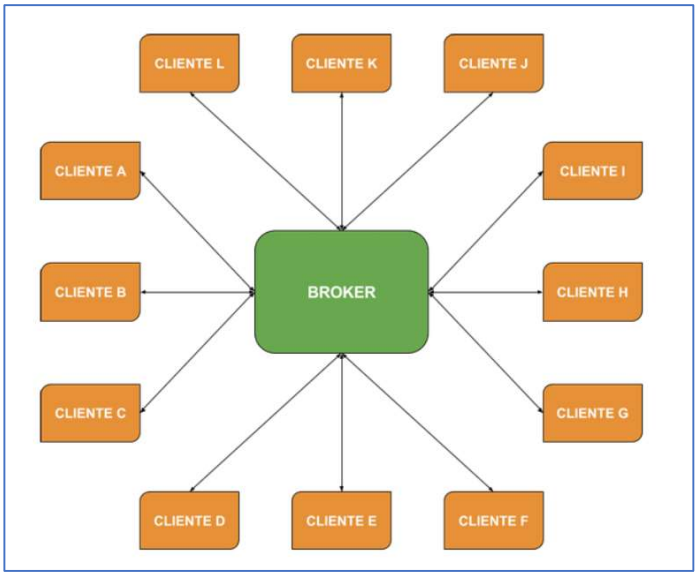


Ilustración 11 - Arquitectura MQTT
Fuente: https://programarfacil.com/esp8266/mqtt-esp8266-raspberry-pi/

Existen 2 tipos de clientes:

- los que publican (conocidos como "*Publishers*")
- los que consumen los datos (denominados "*Suscribers*")

No existe una dependencia entre ellos, ya que no tienen conocimiento de quién está al otro lado. Inclusive podría pasar que no hubieses nadie en el otro extremo.

Esta "no dependencia" es conocida también como desacoplamiento y está dada en 3 dimensiones:

- ***En el espacio***: El publicador y el suscriptor no tienen por qué conocerse.
- ***En el tiempo***: El publicador y el suscriptor no tienen por qué estar conectados en el mismo momento.
- ***En la sincronización***: las operaciones en cualquiera de los dos componentes no quedan interrumpidas mientras se publican o se reciben mensajes.

Cada cliente *MQTT* abre una conexión permanente *TCP* con el *Broker*, ya que este se encarga de gestionar la red y de la administración de los mensajes.

Este tipo de arquitecturas, lleva asociada otra interesante característica: la comunicación puede ser de uno a uno o de uno a muchos. Esto permite algo muy importante en proyectos de este tipo: la escalabilidad.

Concepto "topic"

Es muy relevante el concepto "*topic*" o "tema" (en español) ya que a través de estos "*topics*" se articula la comunicación puesto que emisores y receptores deben estar suscritos a un "*topic*" común para poder entablar la comunicación.

Un "tema" es representado mediante una cadena y tiene una estructura jerárquica, ejemplificada en la siguiente ilustración. Cada jerarquía se separa con "/".

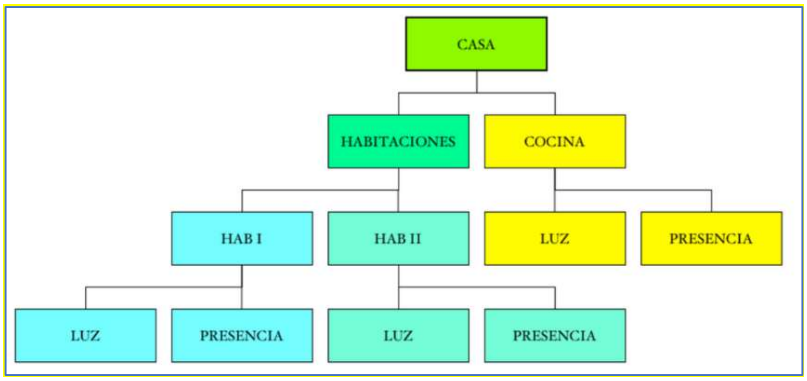


Ilustración 12 - Ejemplo de estructura de sensores en una casa
Fuente: https://ricveal.com/blog/primeros-pasos-mqtt/

Como podemos ver la estructura estaría dada por:

- *Casa/habitaciones/*
  - *Casa/Habitaciones/Hab I*
  - *Casa Habitaciones/Hab II*
- *Casa/Cocina*

Por debajo de ellos ya se encuentran los *topics* propiamente dichos, que son los que producen la información.

Esta estructura permite el uso de comodines para suscribirse, el "+" (reemplaza un único nivel) y el "#" (reemplaza cualquier número de niveles y se lo pone al final).

Ejemplos:

- Si quisiera suscribirme al *topic* "*Luz*" de las habitaciones en un único comando debería consultar el *topic*: *Casa/Habitaciones/+/Luz*
- Si quisiera todos los *topics* de la Habitación I: *Casa/Habitaciones/Hab I/+*
- Si quisiera todos los mensajes de la casa: *Casa/#*

El *Broker* tiene la capacidad de hacer que los mensajes sean persistentes, guardando el mensaje hasta que se conecte el cliente al que va dirigido y es el único que sabe quiénes están suscriptos a cada *topic*

Servicio de Calidad o QoS

El protocolo cuenta con un Servicio de Calidad o *QoS* (del inglés *Quality of Service*). Este servicio determina cómo se entrega el mensaje a los receptores.

El *QoS* se especifica en cada mensaje que se envía y puede haber 3 grados de calidad:

- ***QoS 0***: como máximo una vez. Esto implica que puede que no se entregue. Se lo conoce como "fire & forget"[53].
- ***QoS 1***: al menos una vez. Se garantiza la entrega, pero puede que duplicados.
- ***QoS 2***: exactamente una vez. Se garantiza que llegará una vez el mensaje.

Utilizar un grado de calidad u otro dependerá de la fiabilidad que queramos tener en nuestro sistema. Sin embargo, debes tener en cuenta que cuanta más calidad menor será el rendimiento.

Mensajes

Los mensajes *MQTT* se entregan asincrónicamente ("*push*") a través de la arquitectura "*publish-subscribe", tal como puede observarse en la "ilustración 13"*. El protocolo funciona intercambiando una serie de paquetes de control de una manera definida. Cada paquete de control tiene un propósito específico y cada bit del paquete se crea cuidadosamente para reducir los datos transmitidos a través de la red.

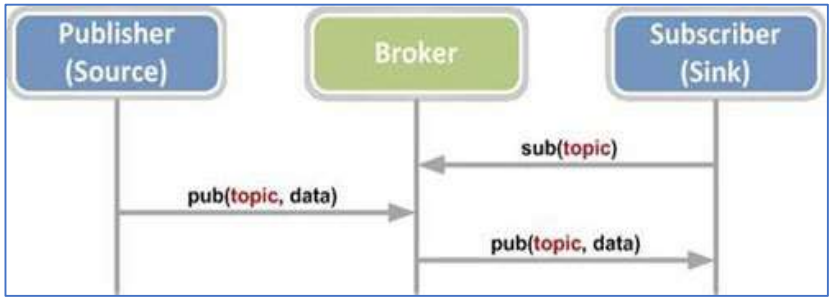


Ilustración 13 - Mensajes de Publish y Subscribe
Fuente: https://aprendiendoarduino.wordpress.com/2018/11/19/mqtt/

[53] **Fire & forget**: Es uno de los más efectivos canales de comunicación asíncronos. No requieren que el origina la comunicación espere hasta que el mensaje se entregue al Destinatario. La conversación no tiene estado porque no hay ningún estado de conversación que deba ser atendido. El manejo de errores no es posible porque no hay comentarios sobre la entrega de mensajes

Una sesión *MQTT* se divide en cuatro etapas:

- conexión,
- autenticación,
- comunicación
- terminación.

Un cliente comienza creando una conexión *TCP/IP* con el *broker* utilizando un puerto estándar o un puerto personalizado definido por los operadores del *broker*. Al crear la conexión, es importante reconocer que el servidor puede continuar una sesión antigua si se le proporciona una identidad de cliente reutilizada.

Seguridad MQTT

Es conocida la importancia de la seguridad, más en escenarios *IoT* en el que comunican objetos entre sí. *MQTT* confía en tecnologías estándares para lograrla:

- Autenticación usuario/*Password*
- Seguridad *SSL/TLS*

Los puertos estándar son el 1883 para la comunicación no cifrada y el 8883 para la comunicación cifrada mediante *SSL/TLS*. Durante el *handshake SSL/TLS*, el cliente valida el certificado del servidor para autenticar el servidor. El cliente también puede proporcionar un certificado de cliente al *broker* durante el *handshake*, que el *broker* puede utilizar para autenticar al cliente. Aunque no forma parte específica de la especificación *MQTT*, se ha convertido en habitual que los *broker* admitan la autenticación de clientes con certificados *SSL/TLS* del lado del cliente.

Dado que *MQTT* pretende ser un protocolo para dispositivos con recursos limitados y de *IoT*, el *SSL/TLS* puede no ser siempre una opción y, en algunos casos, puede no ser deseable, debido a que no es un protocolo ligero.

En estos casos, la autenticación se presenta como un nombre de usuario y contraseña de texto claro que el cliente envía al servidor como parte de la secuencia de paquetes *CONNECT/CONNACK*.

Algunos *brokers*, especialmente los que se encuentran abiertos publicados en Internet, aceptan clientes anónimos. En tales casos, el nombre de usuario y la contraseña simplemente se dejan en blanco.

Reto MQTT: Seguridad, Interoperabilidad y Autenticación

Debido a que el protocolo no fue diseñado con la seguridad en mente, el mismo ha sido tradicionalmente utilizado en redes *back-end* seguras, para propósitos específicos de la aplicación. La estructura temática puede fácilmente formar un árbol enorme, y no hay una manera clara de dividir un árbol en dominios lógicos más pequeños que puedan ser federados. Esto dificulta la creación de una red globalmente escalable porque, a medida que crece el tamaño del árbol temático, aumenta la complejidad.

Otro aspecto negativo de *MQTT* es su falta de interoperabilidad. Debido a que las cargas útiles de mensajes son binarias, sin información sobre cómo están codificadas (sin metadatos), pueden surgir problemas, especialmente en arquitecturas abiertas en las que se supone que las diferentes aplicaciones de los diferentes fabricantes funcionan a la perfección entre sí.

Autenticar clientes con certificados del lado del cliente no es un proceso simple, y no hay manera en *MQTT*, excepto el uso de medios propietarios fuera de banda, para controlar quién posee un *topic* y quién puede publicar información sobre él. Esto hace que sea muy fácil inyectar mensajes dañinos, ya sea intencionadamente o por error, en la red.

Además, no hay forma de que el receptor del mensaje sepa quién envió el mensaje original a menos que esa información esté contenida en el mensaje real. Las características de seguridad que tienen que ser implementadas sobre *MQTT* de forma propietaria aumentan la huella de código (concepto conocido como "*footprint*") y hacen que las implementaciones sean más difíciles.

Protocolo ZigBee

El protocolo ZigBee (Hillman, 2016) es un estándar para redes de área personal inalámbricas (*WPAN*, por sus siglas en inglés)[54] de baja potencia, es decir, redes inalámbricas de corto alcance, generalmente de 10 a 100 metros.

[54] **WPAN**: Una red inalámbrica de área personal. Incluye redes inalámbricas de corto alcance que abarcan un área de algunas decenas de metros. Ejemplo de este tipo de redes son: bluetooth (IEEE 802.15.1) y Zigbee (IEEE 802.15.4)

Está muy difundido dentro del entono de aplicaciones de control y monitoreo inalámbricos, tales como redes de sensores inalámbricos (*WSN*)[55], monitoreo de plantas industriales, control de edificios, hospitales, medición inteligente (M. Nabeel, 2012) y automatización del hogar. En realidad, hay perfiles públicos definidos en la especificación ZigBee para muchos de estos casos de uso.

ZigBee opera en las bandas de radio industriales, científicas y médicas (*ISM*)[56] y la frecuencia exacta dependerá de dónde se encuentre en el mundo. Puede usar la banda de 868 MHz en gran parte de Europa, 915 MHz en los Estados Unidos y 2.4 GHz en muchos otros lugares.

Esta última comúnmente utilizada debido a que existen muchos conjuntos de chips disponibles que la utilizan.

Las velocidades disponibles dependen de la banda que esté utilizando, pero el máximo es de 250 Kbps. Esto es más lento que otras tecnologías inalámbricas populares como *WiFi*, pero también con equipos más económicos y de menor costo operacional.

¿Cómo opera ZigBee?

La base de ZigBee es la especificación 802.15.4 que define las capas Física (*PHY*) y Control de acceso al medio (*MAC*) para *WPAN* de baja velocidad (*LR-WPAN*)[57]. ZigBee agrega capas sobre esto para agregar más inteligencia de red y aplicación.

Una red que use este protocolo le permite a un conjunto de dispositivos se comuniquen de forma inalámbrica a través de una de las varias topologías posibles. Los paquetes de datos se pueden enviar entre nodos y los dispositivos intermediarios pueden enrutarlos a nodos más distantes que, de lo contrario, estarían fuera del alcance. Los paquetes pueden protegerse mediante cifrado, pero para que esto funcione, todos los nodos necesitarán una clave y, como

[55] **WSN**: Redes de sensores inalámbricos (en inglés, Wireless sensor networks), también llamadas redes de sensores y actuadores (Wireless sensor and actuator networks, WSAN). Son sensores autónomos espacialmente distribuidos para monitorizar condiciones físicas o ambientales, como temperatura, sonido, presión, etc. y para pasar sus datos de forma cooperativa sus datos a través de la red a otras ubicaciones

[56] **Banda ISM**: Las bandas de radio industriales, científicas y médicas (ISM) son bandas de radio (partes del espectro de radio) reservadas internacionalmente para el uso de energía de radiofrecuencia (RF) para fines industriales, científicos y médicos distintos de las telecomunicaciones. Los ejemplos de aplicaciones en estas bandas incluyen el proceso de calentamiento por radiofrecuencia, hornos de microondas y máquinas de diatermia médica. Las potentes emisiones de estos dispositivos pueden crear interferencias electromagnéticas e interrumpir las comunicaciones de radio utilizando la misma frecuencia, por lo que estos dispositivos se limitaron a ciertas bandas de frecuencias. En general, los equipos de comunicaciones que operan en estas bandas deben tolerar cualquier interferencia generada por las aplicaciones ISM, y los usuarios no tienen protección regulatoria contra la operación del dispositivo ISM.

[57] **LR-WPAN**: Las redes de área personal inalámbrica de baja velocidad (Low Rate - WPAN) que se especifican en IEEE 802.15.4 y que operan en la banda ISM de 2,4 GHz se utilizan ampliamente en edificios y hogares inteligentes, y también en automatización industrial.

será expuesto más adelante, puede haber problemas en torno a cómo se implementan dichas claves en los dispositivos.

Identificación de la red

Cada red ZigBee tiene su propio identificador, conocido como *ID PAN* (*Id Personal Area Netwok*).

Zig Bee Stack

En la siguiente ilustración son presentadas cada una de las capas del protocolo:

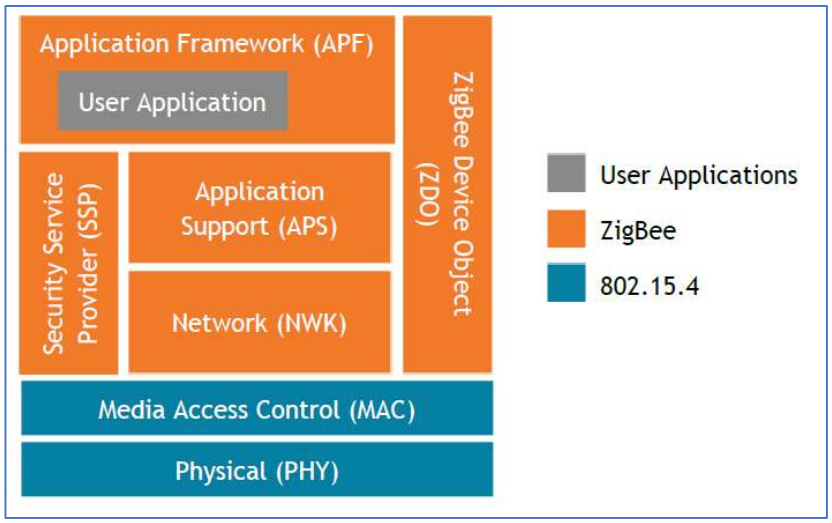


Ilustración 14 - Stack del protocolo ZigBee
Fuente: https://www.mwrinfosecurity.com/assets/Whitepapers/mwri-zigbee-overview-finalv2.pdf

PHY: Capa física. Responsable de la modulación, demodulación y transmisión física de paquetes por el aire y maneja varias cosas necesarias para una transmisión de radio robusta en entornos ruidosos y propensos a interferencias. Definida por 802.15.4.

MAC: Control de Acceso al Medio. Realiza funciones como *CSMA/CA*[58] para evitar colisiones al transmitir tramas y define un formato de trama con cosas como direcciones *MAC*, etc. Esta capa también define topologías de red sobre las que ZigBee se basa y mejora en niveles más altos de la pila. También definido por 802.15.4

NWK: Red. Proporciona la capacidad de descubrir y unirse a redes y se expande en las topologías definidas por 802.15.4 en la capa *MAC* para permitir redes de malla, una característica popular de ZigBee. También determina rutas a través de la red ZigBee y admite

[58] **CSMA/CA** (del inglés *Carrier Sense Multiple Access with Collision Avoidance*) o, en español, acceso múltiple por detección de portadora y prevención de colisiones, es un protocolo de control de acceso a redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión.

direcciones ZigBee que son diferentes a las direcciones *MAC* presentes en la capa *MAC* basada en 802.15.4.

APS: Soporte de Aplicaciones. A cargo de implementar las funciones que necesitan las aplicaciones de ZigBee y que actúa como una interfaz para la capa *NWK*. Realiza un filtrado de paquetes duplicados desde la capa *NWK* y mantiene una tabla de enlace de nodos en la red.

SSP: Proveedora de Servicios de Seguridad. Encargada de proporcionar servicios de seguridad ZigBee a las capas *NWK* y *APS*, incluidos el establecimiento y transporte de claves, la gestión de dispositivos y la protección de tramas.

ZDO: Objetos Dispositivos ZigBee. Capa responsable de la administración general del dispositivo ZigBee. El *ZDO* inicializa la capa *APS* y *NWK*, permite el descubrimiento del dispositivo, gestiona las solicitudes de enlace y define el modo del dispositivo (coordinador, enrutador o dispositivo final).

APF: Framework de Aplicaciones. Es un entorno de ejecución para las aplicaciones de usuario de ZigBee y facilita el envío y la recepción de datos por parte de esas aplicaciones. También proporciona un punto final para cada aplicación, con el punto extremo 0 reservado para el *ZDO* y el punto extremo 255 para una dirección de difusión. Las aplicaciones implementan la función del dispositivo ZigBee (por ejemplo, un sensor).

Tipos de Nodos ZigBee

Hay tres tipos de nodos en los que un dispositivo puede actuar dentro de una red ZigBee:

- **Coordinador**: Cada red ZigBee debe tener un único Coordinador. Este nodo es el primer nodo en iniciarse e inicializa el resto de la red, seleccionando la frecuencia a utilizar, el *ID PAN* de la red y permitiendo que otros nodos se unan a la red. Actúa como el padre de los nodos que se conectan a la red a través de ella (sus hijos). El Coordinador también suele ejecutar otros servicios como enrutamiento y ciertos servicios de seguridad.
- **Enrutador**: Son responsables de retransmitir mensajes a otros nodos. Aunque los enrutadores no son necesarios en todas las topologías ZigBee, pero aún se encuentran comúnmente. Dependiendo la tipología, como se describe más adelante, los nodos también pueden unirse a la red a través de un enrutador, con el

enrutador convirtiéndose en su nodo principal; Esto puede incluir que un enrutador sea el padre de otro enrutador.

- **Dispositivo final**: Nodo simple que envía y recibe mensajes, pero no realiza ninguna otra función especial en la red.

Topología de red ZigBee

Las redes ZigBee pueden presentar tres topologías diferentes que definen la forma en las cuales son enrutados los mensajes y cómo es la comunicación entre los dispositivos.

Estrella

Es la topología más simple y limitada disponible para ZigBee, representada en la siguiente ilustración. Todos los dispositivos se conectan a un nodo Coordinador y toda la comunicación se realiza a través de éste.

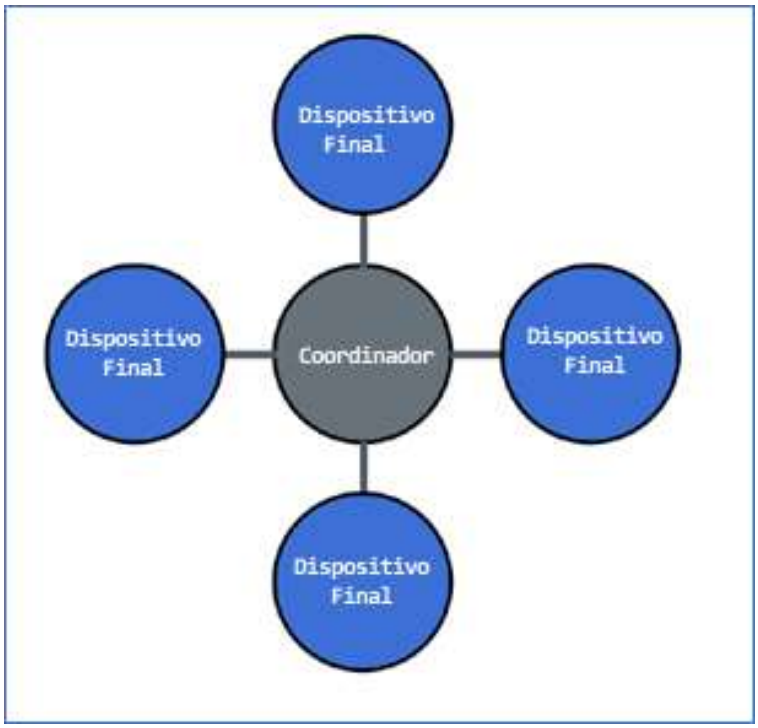


Ilustración 15 - ZigBee. Topología Estrella
Fuente: https://www.mwrinfosecurity.com/assets/Whitepapers/mwri-zigbee-overview-finalv2.pdf

Con esta topología, el rendimiento de la red está limitado por el Coordinador y, si el éste falla, la red completa falla. El alcance de la red también se encuentra limitado al alcance que éste posea.

Árbol

En esta topología, el Coordinador forma el nodo raíz de un árbol de nodos secundarios, graficada en la "ilustración 16". Los Nodos hoja pueden ser dispositivos finales o enrutadores a los cuales no se les hayan unido nodo hijos. Los nodos intermedios son enrutadores. La comunicación directa sólo puede ocurrir entre un nodo secundario y su padre, pero todos los nodos pueden comunicarse juntos mediante mensajes que atraviesan el árbol hasta un antepasado común y luego hacia el nodo objetivo.

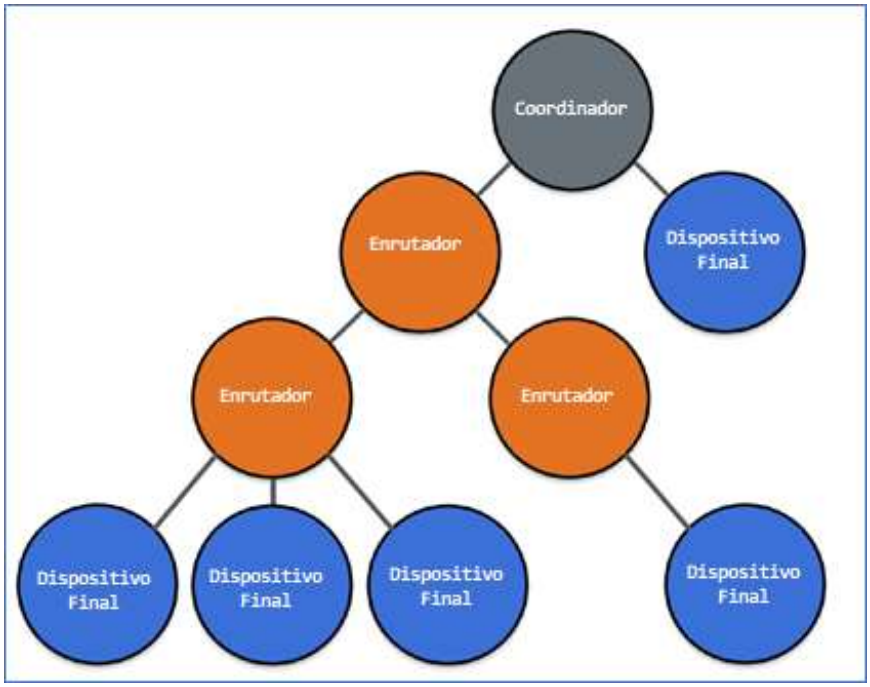


Ilustración 16 - ZigBee. Topología Árbol
Fuente: https://www.mwrinfosecurity.com/assets/Whitepapers/mwri-zigbee-overview-finalv2.pdf

Con esta configuración, los enrutadores pueden ampliar el alcance de la red más allá de cualquier enlace de dispositivo a dispositivo.

Sin embargo, si un enrutador falla, no hay una ruta alternativa y algunas partes de la red pueden desconectarse.

Malla

Esta topología es la más flexible que ofrece ZigBee, representada en la "ilustración 17". Es similar a la topología de árbol, pero sin seguir su estructura rígida ya que permita la comunicación entre enrutadores o con el coordinador si está dentro del rango. Esto significa que puede haber muchas rutas diferentes a través de la red a un nodo determinado, y ZigBee

tiene una función de descubrimiento de ruta para encontrar la mejor ruta a un nodo determinado y, por lo tanto, puede ser "autorreparable".

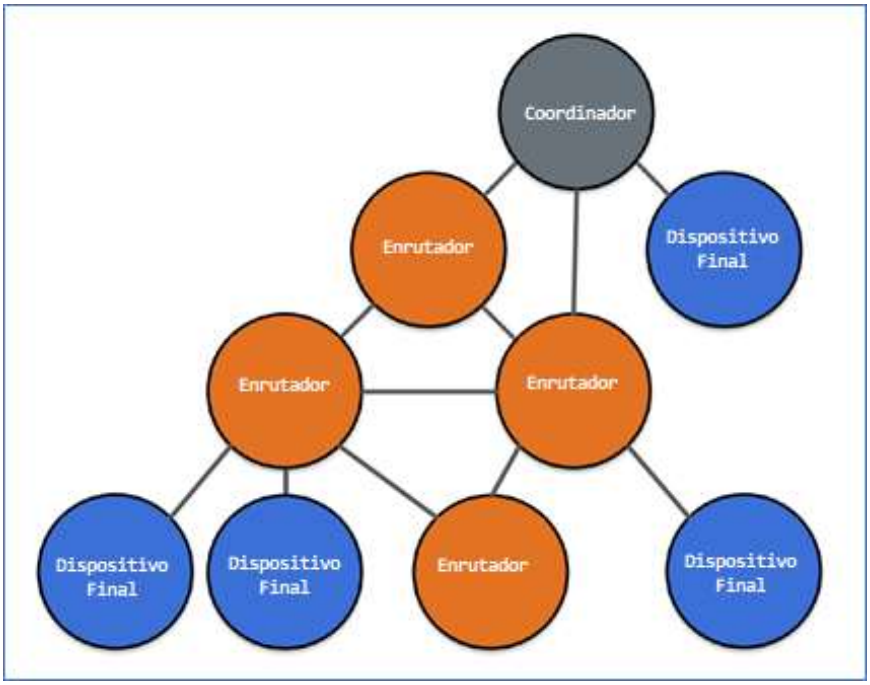


Ilustración 17 - ZigBee. Topología Malla
Fuente: https://www.mwrinfosecurity.com/assets/Whitepapers/mwri-zigbee-overview-finalv2.pdf

En la siguiente imagen es evidenciada una típica topología de malla, implementada para la medición de consumos residenciales en un barrio.

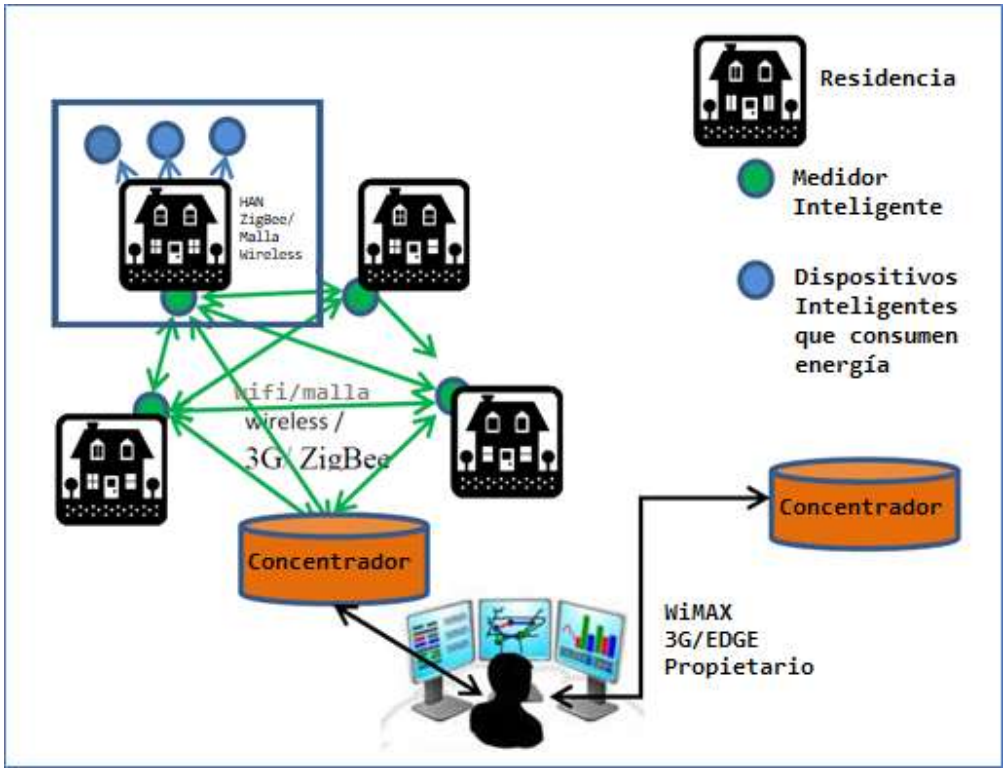


Ilustración 18 - ZigBee. Topología de Malla para medición de consumo residencial
Fuente: https://arxiv.org/ftp/arxiv/papers/1206/1206.3880.pdf

Cómo se propagan los mensajes de ZigBee

Los mensajes de ZigBee pueden enviarse a un nodo específico, a un grupo de nodos, o transmitirse a (potencialmente) todos los nodos e incluso pueden enviarse entre redes ZigBee con diferentes *ID PAN*.

Transmisión: Cuando se envía una transmisión, cualquier Coordinador o Enrutador dentro del alcance lo retransmitirá a menos que haya alcanzado el número máximo de retransmisiones. Esto significa que una transmisión sólo puede propagar un cierto número de saltos antes de que deje de enviarse.

Los mensajes de difusión se identifican cuando la dirección de red se establece en una de las direcciones de difusión predefinidas. El más común es *0xFFFF* que se transmite a todos los dispositivos, pero también existen las siguientes direcciones:

- *0xFFFD* - Transmisión a todos los dispositivos con el receptor encendido permanentemente
- *0xFFFC* - Difusión a todos los enrutadores y coordinadores
- *0xFFFB* - Difundir a enrutadores de baja potencia

Unicast: los mensajes de *unicast* se dirigen hacia un único nodo. Obviamente, no todos los nodos pueden comunicarse directamente, dependiendo del rango de transmisión y la topología de la red, por lo que los mensajes a menudo pasan por múltiples nodos hasta llegar a su destino final.

Multidifusión de grupo: se utiliza para enviar un mensaje simultáneamente a un grupo de nodos. Los mensajes se envían con una dirección del grupo, debiendo estar configurado para tal fin.

Transferencia enlazada: se produce cuando se envía un mensaje a los puntos finales a los que se ha vinculado el remitente.

Transferencia Inter-PAN: esto es cuando un mensaje se envía a un nodo en una red con una *ID PAN* diferente.

Como fuera descrito anteriormente, el estándar 802.15.4 admite el direccionamiento *inter-PAN* y, aunque no es realmente parte de ZigBee, algunos dispositivos lo admiten.

Por lo general, estos mensajes no se reenvían ni se enrutan a través de la red y simplemente se envían directamente a un dispositivo fuera de la red que está dentro del alcance del remitente.

Esto puede permitir cierta transferencia de datos a otros dispositivos que pueden no ser compatibles con toda la red. Es importante destacar que estas transmisiones no están cifradas, ya que están destinadas a una red externa fuera del marco de seguridad normal. Por supuesto, podría ser posible para los desarrolladores agregar cifrado a nivel de aplicación usando una clave compartida o similar.

Para los mensajes que necesitan pasar por varios nodos para llegar a su destino final, se usan dos campos de dirección; "Siguiente salto" y "destino final". El siguiente salto está determinado por una tabla de enrutamiento mantenida por cada nodo de enrutador o coordinador y se completa cada vez que uno de estos nodos reenvía un paquete. En el caso de que no se encuentre una entrada en la tabla de enrutamiento, será utilizado el mecanismo de descubrimiento de ruta por medio de mensajes de difusión.

Seguridad

Centro de Confianza

El Centro de Confianza es un dispositivo en el que confían todos los dispositivos dentro de una red ZigBee para distribuir claves con el fin de la administración de la configuración de la red y de la aplicación de extremo a extremo.

Sólo hay un Centro de Confianza en una red ZigBee. Suele ser, por lo general, el nodo Coordinador.

Claves

ZigBee usa una jerarquía de claves para administrar la seguridad. Hay tres tipos de claves: Enlace (*Link*), Red (*Network*) y Maestra (*Master*).

> **Clave de Enlace**: Es compartida, de forma única, entre dos dispositivos y se puede usar para cifrar mensajes de unidifusión entre ellos. Si un dispositivo comparte una Clave de Enlace con el Centro de Confianza, puede utilizarse para cifrar la transferencia de la Clave de Red a un nodo que se une a la red.
>
> Otras Claves de Enlace operan en la capa *APS* y se conocen como Claves de Enlace de capa de aplicación.
>
> Las Claves de Enlace se comportan como claves de sesión secretas utilizadas entre dos dispositivos ZigBee que se comunican y son exclusivas de esos dispositivos. Las claves de enlace se utilizan para proteger los mensajes de unidifusión entre dos dispositivos en la Capa de Aplicación.
>
> **Clave de Red**: Es compartida entre todos los dispositivos conectados en la red y puede ser utilizada para el cifrado de capa *NWK* y para proteger el tráfico de difusión. Un conjunto de claves de red se almacena en el Centro de Confianza y se identifica mediante un número de secuencia de clave.
>
> Las mismas pueden preinstalarse en dispositivos o transportarse desde el Centro de Confianza. Dicho transporte sólo se cifrará si hay otra clave disponible para ser utilizada como Clave de Transporte de dicha clave, como puede ser la Clave de Enlace del Centro de Confianza.

La Clave *Network* se utiliza para realizar la seguridad de la capa de red (mensajes de enrutamiento, solicitudes de combinación de red, etc.) y para evitar la unión y el uso no autorizados de la red ZigBee.

Todos los dispositivos en una red ZigBee comparten la misma clave de Network. Cuando uno o más dispositivos se ven comprometidos y esta es filtrada, hay una ventana de vulnerabilidad hasta que se establezca una nueva.

El Centro de Confianza tiene un conjunto de Claves de Red y la clave de red actual, identificadas mediante un número de secuencia de claves.

El Centro de Confianza puede actualizar periódicamente y cambiar a una nueva clave de Network. La nueva es cifrada con la antigua y es transmitida. Los dispositivos se envían mensajes para cambiar a la nueva clave.

Las claves de red del Centro de confianza se pueden preinstalar

Clave Maestra: utilizada para el establecimiento de claves de enlace *SKKE*[59]. Por lo general, preinstalados, algunos mecanismos pueden usar una "clave de carga de claves" para ayudar a transferir de manera segura una Clave Maestra del Centro de Confianza a un dispositivo.

Estas claves también proporcionan la base para la autenticación a través de un mecanismo de respuesta de un desafío.

ZigBee PRO también admite la Autenticación de entidad de clave simétrica mutua entre cualquier dispositivo, así como también la autenticación a la red en su conjunto.

La Clave *Master* es un secreto compartido inicial entre dos dispositivos que realizan el procedimiento de establecimiento de clave para generar las claves de enlace.

La Clave Maestra puede preconfigurarse o proporcionarse desde el Centro de Confianza. Al poseer una Clave de Red correcta, un nodo puede utilizar la red para recibir y transportar datos. Observe que la Clave de *Network* proporciona una verificación de seguridad para utilizar la red. Para proporcionar la autenticación del nodo de origen se debe generar y utilizar la Clave de *Link* (clave criptográfica de extremo a extremo) como una medida de protección de seguridad adicional.

[59] **SKKE**: establecimiento de clave simétrica, detallado más adelante

Esta clave es exclusiva de un par de dispositivos que se comunican entre sí y se deriva de sus respectivas Claves Maestras.

Creación/Instalación de claves

Las claves pueden ser instaladas de tres maneras distintas: "fuera de banda", "dentro de banda" o "precargadas de fábrica".

"Fuera de banda": La carga las claves es llevada a cabo por medio de mecanismos distintos a los canales operativos normales de la red, por ejemplo, a través de un puerto serie en el dispositivo ZigBee conectado a una computadora portátil.

"En banda": La entrega la clave es completada por medio de un canal de comunicación "normal". Hay una pequeña ventana de vulnerabilidad en la que el dispositivo no configurado no está protegido.

"Precargadas de fábrica": La clave pueden ser configuradas en fábrica. Luego, la clave es transmitida al cliente, de manera segura (al menos así debería ser). Además, en este caso, el proveedor tiene conocimiento de la clave del cliente.

Desde el punto de vista de seguridad, la carga de la clave "fuera de banda" generada por el cliente sería el método más seguro.

La Clave *Master*, la dirección del Centro de Confianza y las allí almacenadas podrían preinstalarse.

Hay tres modos de establecer una clave:

- Establecimiento de clave simétrica (*SKKE*[60]),
- Establecimiento de clave pública (*PKKE*[61])
- Establecimiento de clave basado en certificado (*CBKE*[62]).

El *SKKE* produce la clave de enlace basada en un secreto compartido, la Clave Maestra. Si ésta se encuentra comprometida, se conoce públicamente o se establece en el valor predeterminado, la Clave de Enlace establecida también estará comprometida.

[60] **SKKE**: Symetric-Key Key Establishment
[61] **PKKE**: Public-Key Key Establishment
[62] **CBKE**: Certificate-Based Key Establishment

El *PKKE* se basa en una clave pública estática o temporal compartida. Una clave pública no necesita mantenerse en secreto, por lo que su conocimiento no compromete la Clave de Enlace. Dependiendo del método, la clave pública se vinculará a un dispositivo, ya sea transportado de forma independiente o como parte del certificado de autenticación, es *PKKE* o *CBKE*.

El *CBKE* proporciona la forma más completa de establecimiento clave. Se basa en el uso de los certificados implícitos de curva elíptica Qu-Vanstone (*ECQV*[63]) que son mucho más pequeños en tamaño que los certificados convencionales. Cada uno de estos certificados enlaza una dirección *MAC* de dispositivo y un identificador de fabricación a un par de claves *ECC*[64].

Este método funciona de manera similar al protocolo de intercambio de claves Diffie-Hellman[65], excepto que las claves públicas de los dos dispositivos no se intercambian, sino que sus certificados correspondientes se usan para derivar las claves públicas entre sí.

Modos de Operación

ZigBee provee dos modos de operación:

- Modo de Seguridad Estándar (también llamado “Residencial”)
- Modo de Alta Seguridad (también llamado “Comercial”).

Estos modos afectan la distribución, en el caso de existir, el almacenamiento y el cifrado de las claves.

Modo Residencial

La lista de dispositivos, Claves Maestras y Claves de Red puede ser mantenida por el Centro de Confianza o por los propios dispositivos.

La responsabilidad del Centro de Confianza es mantener una Clave de Red y actuar como la autoridad central para admitir nodos en la red.

[63] **ECQV**: Algoritmo de cifrado que utiliza curvas elípticas. Especificado en el documento Normas para la criptografía eficiente http://www.secg.org/sec4-1.0.pdf

[64] **ECC**: Criptografía de Curva Elíptica (del inglés: *Elliptic Curve Cryptography,* ECC) es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas

[65] **Diffie-Hellman**: El protocolo criptográfico de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro y de manera anónima (no autentificada).
Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión (establecer clave de sesión). Siendo no autenticado, sin embargo, provee las bases para varios protocolos autenticados.
Los autores fueron Whitfield Diffie y Martin Hellman

La seguridad de la aplicación se proporciona a través de una única Clave de Red, tal como es graficado en la "ilustración 19".

Cada modo puede identificar lo que está cifrado y la longitud de la clave. También se pueden establecer contadores de *frames*[66] proporcionados por la fuente para protegerlos de una amenaza de reproducción. Además, un campo Identificador de clave puede especificar la clave necesaria para comunicarse con un nodo.

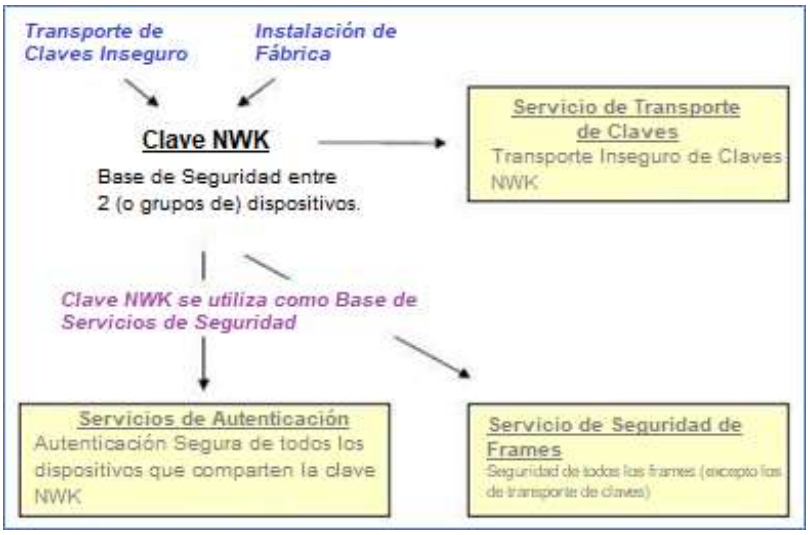


Ilustración 19 - ZigBee. Uso de Claves en Modo Residencial
Fuente: https://arxiv.org/ftp/arxiv/papers/1206/1206.3880.pdf

Modo Comercial

En el modo comercial, el Centro de Confianza mantiene claves (Maestra, Red y Enlace) para cada dispositivo de red, lo que permite el control y mantenimiento centralizados de las claves. En este modo, el costo de la memoria aumenta según el tamaño de la red.

La Clave Maestra es una clave secreta entre dos nodos y es el punto de partida para establecer la Clave de *Link*. El establecimiento de esta última es procesado por el protocolo *SKKE*, situación representada en la "ilustración 20".

La clave de enlace es compartida por dos dispositivos y la Clave de Red se comparte entre todos los dispositivos.

[66] **Frame**: Un paquete de datos o simplemente paquete, que es un bloque fijo de datos transmitidos como una sola entidad. También se lo conoce como trama.

Para realizar el transporte de la Clave de Red, se utiliza una clave adicional derivada de una Clave de Enlace para proteger los mensajes de transporte de claves que llevan una clave que no sea una Clave Maestra (servicio de transporte de claves).

La diferencia entre las Claves de Red residencial y comercial está en las reglas utilizadas para su distribución.

Una Clave de Red comercial nunca puede enviarse sin cifrar a través del aire, mientras que en el modo residencial esto está permitido. Para transportar de forma segura entre el Centro de Confianza y un dispositivo, dicho Centro cifra la clave mediante una Clave de Enlace basada en el algoritmo *AES*[67] y los datos así son enviados cifrados. El dispositivo descifra los datos enviados utilizando la Clave de Enlace, que es idéntica para las operaciones de cifrar y descifrar un mensaje.

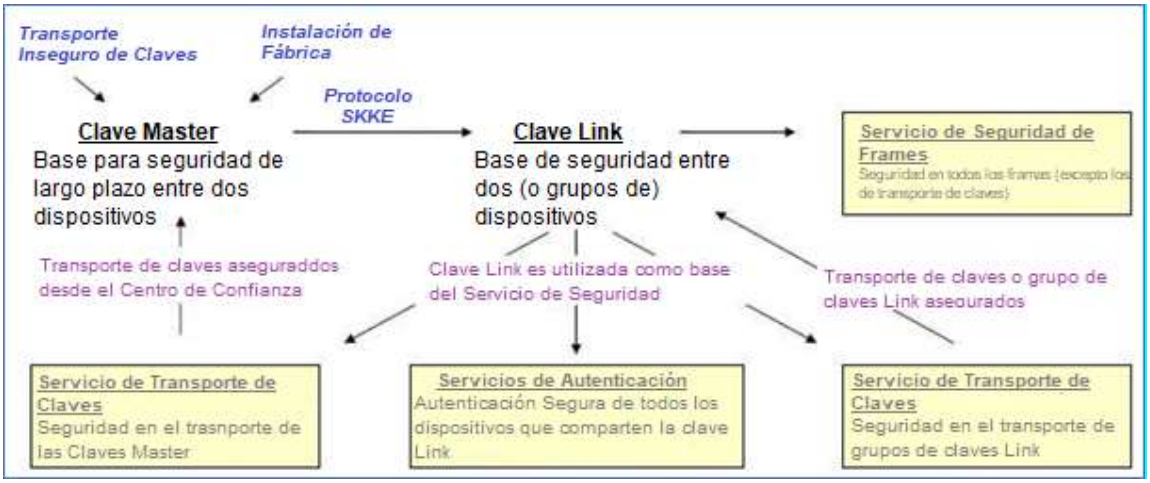


Ilustración 20 - ZigBee. Uso de Claves en Modo Comercial
Fuente: https://arxiv.org/ftp/arxiv/papers/1206/1206.3880.pdf

Cifrado, Integridad y Autenticación

Como cualquier red inalámbrica donde la seguridad es una preocupación, el cifrado juega un papel importante.

Existe un buen número de opciones de seguridad que pueden configurarse que afectan el cifrado en una red ZigBee, y la forma en que se administran e intercambian las claves que puede ser definido, en parte, por el Perfil de la aplicación que se está utilizando y si la red está utilizando el modo de seguridad estándar o el modo de alta seguridad.

[67] **AES**: *Advanced Encryption Standard*, también conocido como Rijndael. Es un algoritmo de cifrado simétrico con un esquema de cifrado por bloques. Adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

En última instancia, el cifrado se puede aplicar en tres niveles diferentes:

- En la capa de control de acceso al medio (*MAC*),
- En la capa de red (*NWK*)
- En la capa de soporte de aplicaciones (*APS*)

Un marco ZigBee contendrá campos de todas estas capas encapsuladas entre sí, y cada una tiene la posibilidad de cifrar su carga útil de datos.

Todo el cifrado en una red ZigBee utiliza *AES*-128[68], incluso en el nivel 802.15. 4. que proporciona cifrado simétrico, lo que significa que ambas partes deben compartir una clave.

La manera en la cual los nodos obtienen estas claves es un problema de seguridad importante. Hay tres métodos principales que un nodo puede obtener claves:

Preinstalación: las claves se colocan en dispositivos fuera de banda (por ejemplo, programados físicamente antes de la implementación).

Transporte: las claves se transportan a través de la red al dispositivo.

Establecimiento: a través de un proceso de negociación, las claves se establecen sin enviarlas a través de la red. Tres métodos de establecimiento son:

- Establecimiento de clave simétrica (*SKKE*)
- Establecimiento de claves basadas en certificados (*CBKE*)
- Establecimiento de clave Alpha-Secure (*ASKE*)

Donde las claves no están preinstaladas, debe haber un dispositivo que pueda almacenar y distribuir o negociar claves. Esto será puesto en marcha por el Centro de Confianza.

Ésta también autentica los dispositivos en la red. Cuando se usan varias claves, es posible distribuir algunas claves de forma segura, pero hay situaciones en las que ZigBee puede configurarse de manera que las claves se envíen sin cifrar a través de la red, lo que introduce un breve período de vulnerabilidad.

También se usa un contador de *frames* que se incrementa con cada transmisión. Esto ayuda a evitar ataques de repetición y forma parte de un valor único que garantiza la frescura de la trama con respecto a la criptografía. Si un dispositivo recibe un *frame* con un contador de

[68] **AES-128**: Implementación del algoritmo AES, con un tamaño de bloque de 128 bits.

estos más bajo que el valor anterior, lo rechazará. El contador de tramas también está asociado a la Clave de Red actual, y el Centro de Confianza cambiará periódicamente la Clave de Red y restablecerá dicho contador en cero para evitar bloquear la red cuando el contador alcance su valor máximo. La Clave de Red debe cambiarse para restablecer el contador de tramas.

Si bien el cifrado puede proporcionar la confidencialidad de los datos que se transmiten y permitir la autenticación, también puede ser utilizado para proporcionar garantías sobre la integridad del mensaje.

Para lograrlo, utiliza el Código de Integridad del Mensaje (*MIC*)[69], también conocido como el Código de Autenticación del Mensaje (*MAC*)[70], que no debe ser confundido con la capa *MAC* en la pila de protocolos ya mencionados.

El *MIC* usa *AES* para firmar efectivamente el mensaje para asegurar que el contenido no haya sido manipulado.

ZigBee puede operar en una serie de configuraciones con respecto al nivel de encriptación y puede habilitarse o deshabilitarse junto con el *MIC*, independientemente del nivel de seguridad.

También permite especificar valores sobre la cantidad de bits que contiene el *MIC*, donde uno más largo se considera más seguro y difícil de forzar o adivinar por un atacante. El tamaño del mismo puede ser de 32, 64 o 128 bits.

Dentro de este esquema, se presentan 2 situaciones a tener en cuenta:

- Cualquier mensaje *Inter-PAN* entre redes no se cifrará, ya que están fuera de los procesos normales de administración de claves dentro de una red ZigBee, como hemos visto anteriormente
- La gestión adecuada de las claves es importante para mantener la seguridad de una red ZigBee y los implementadores deben ser conscientes de que hay situaciones en las que las claves pueden transmitirse de forma clara, lo que abre una ventana de vulnerabilidad a la red.

[69] **MIC**: del inglés Message Integrity Code (Código de integridad de mensajes) en ZigBee es utilizado para verificar que no sea manipulada la información contenida en el mensaje.
[70] **MAC**: del inglés Message Authentication Code (Código de Autenticación del Mensaje). Es una porción de información utilizada para autenticar un mensaje. Los valores MAC se calculan mediante la aplicación de una función hash criptográfica con clave secreta K, que sólo conocen el remitente y destinatario, pero no los atacantes. Se dice que la función hash tiene que ser criptográfica porque tiene que cumplir ciertas propiedades de seguridad que las hacen resistentes frente ataques de adversarios.

5. Riesgos asociados

Cuando un objeto comienza a formar parte de un entorno interconectado, se debe considerar que la seguridad física o lógica puede ser vulnerada por atacantes desde cualquier lugar. Así los atacantes podrían interceptar, leer o modificar información, manipular los sistemas de control y/o modificar alguna funcionalidad del objeto o sistema en el cual se encuentra incorporado. Además, mientras más dispositivos se agreguen a la red, más vulnerable será, ya que crece la superficie de ataque y las oportunidades para hacer daño.

También debe ser tenido en cuenta que toda la información recopilada sobre las personas podría ser tratada y utilizada por terceros para establecer perfiles, gustos, preferencias o hábitos de consumo para obtener beneficios.

Profundizando, pueden clasificarse algunos riesgos/problemas según el entorno en el cual se presentan:

Aspectos Físicos:

- ***Acceso Físico***: se puede manipular/obtener/destruir la información almacenada/recolectada en los dispositivos (tarjetas de memoria o *EEPROM*[71]). Entre los cuales, puede haber contraseñas
- ***Obsolescencia de componentes***: Dispositivos quedan limitados en prestaciones, hablando de seguridad, sobre todo, para prestar servicios. Posiblemente, la cantidad que hayan sido desplegados hará que sigan conviviendo un tiempo "extra" en las redes, haciéndolas más vulnerables.
- ***Componentes con vulnerabilidades conocidas***: Componentes muy utilizados en sensores tienen vulnerabilidades conocidas, como por ejemplo el Texas Instruments CC2430[72], que incluso aparecen en las hojas de datos. Este chip era utilizado dentro de los cálculos de números pseudo aleatorios.
- ***Acceso de los Operadores de Servicios***: Los encargados de instalar y/o mantener los dispositivos en funcionamiento podrían acceder a los datos almacenados.

[71] **EEPROM**: Corresponde a "*Erasable Programmable Read Only Memory*" que se puede traducir como Memoria programable borrable de sólo lectura. También es conocida como "*non-volatile memory*" o memoria no volátil y es debido a que cuando se desconecta la energía, los datos almacenados en la EEPROM no serán eliminados quedando intactos.
[72] **Texas Instruments CC2430**: "*System-on-Chip Solution for* 2.4 GHz IEEE 802.15.4 / ZigBee". Según el propio fabricante ya no es recomendado para nuevos diseños. (www.ti.com/product/cc2430)

- ***Manipulación de los usuarios finales*:** Si la implementación de la red utilizara, por ejemplo, tarjetas *SIM*[73], estas podrían ser robadas / reemplazadas siendo utilizadas para otro fin. (Chan, 2011)

Aspectos Lógicos:

- ***Problemas con autenticación propiamente dicha***: La autenticación básicamente estaría cubierta por credenciales, usuario y contraseña, que muchas veces van en texto claro, al menos por ventanas de tiempo. Esta situación permite la explotación de múltiples posibilidades:
  - Suplantación de Identidades de los dispositivos,
  - Divulgación de información,
  - Ataques Sybil.[74]

Problemas con los algoritmos:

- ***Problemas con los protocolos***: Algunos intercambios de claves, ejemplo en ZigBee, pueden generar ventanas de tiempo vulnerables, al enviarse en texto claro. Esto ocurre, por ejemplo, cuando un nodo es agregado a la red. Todos los componentes de una misma red tienen la misma contraseña de red para poder conectarse a la misma.

  En *MQTT*, sería necesaria la implementación de tráfico con *TLS*, que no sería la implementación por defecto, para que las credenciales sean "protegidas"

- ***Componentes "Fuera de Servicio"***: Cuando un nodo abandona la red, ya sea por mantenimiento, pérdida o compromiso del mismo, el nodo todavía podría acceder a la red si utilizara la información que tiene almacenada si no se hizo una correcta revocación del mencionado nodo.
- ***Problemas con el intercambio de información***: ZigBee permite la comunicación entre redes con distintos identificadores de red (*IP PAN*). La comunicación entre ellas es en texto claro.

[73] **Tarjeta SIM** (acrónimo en inglés de *Subscriber Identity Module*, en español módulo de identificación de abonado) es una tarjeta inteligente desmontable usada en teléfonos móviles, módems HSPA o LTE y otros dispositivos que se conectan por medio de una ranura lectora o lector SIM. Las tarjetas SIM almacenan de forma segura la clave de servicio del suscriptor usada para identificarse ante la red, de forma que sea posible cambiar la suscripción del cliente de un terminal a otro simplemente cambiando la tarjeta.

[74] **Ataque Sybil**: un atacante puede contaminar un sistema distribuido creando un gran número de identidades que aparenten ser independientes y usarlas para obtener una influencia desproporcionada, alterar rutas o modificar contenido almacenado de forma redundante. De esta forma ciertos nodos legítimos pueden sufrir una usurpación de identidad al estar solo conectados a los del atacante. La vulnerabilidad del sistema depende de la facilidad para crear nuevas identidades y la (falta de) importancia de la cadena de confianza, que puede hacer que todas las identidades sean tratadas por igual.

- ***Dificultades con credenciales***: Aparecen problemas tales como
    - Administrar gran número de nombres de usuarios y contraseñas de los dispositivos,
    - Protección de las contraseñas almacenadas en los dispositivos,
    - Administración de las contraseñas durante el ciclo de vida del dispositivo.

CAPITULO III – De la situación problemática a la solución

(Página en blanco)

Introducción

De manera general, en el capítulo anterior, han sido listados problemas que tienen los 2 protocolos más usados en *IoT*.

Éstos están siendo analizados por distintas organizaciones e investigadores, que organizan y difunden la información para que tomen conciencia todos los participantes necesarios en esta tecnología: fabricantes, programadores, implementadores, usuarios de empresas y usuarios finales.

Es entendible que, si bien no son una solución definitiva, permiten acercarse a un estado más seguro, si es tenido en cuenta en el entorno actual.

Debería que comenzase a calificar/evaluar/comparar las instalaciones realizadas o a realizar contra estos *framewoks* de trabajos o bases de datos de manera de corregir, lo más anticipadamente posible los despliegues, existentes y futuros, de la tecnología y, de ser necesario, preparar todos los planes de contingencia y/o contención hasta que puedan ser mitigados los riesgos y corregidas las vulnerabilidades.

Estándares para el control

Diferentes organismos, comunidades, organizaciones sin fines de lucro u objetivo comercial han estado trabajando, y continúan aún, para establecer parámetros a analizar, verificar y entender (entre otras cosas) los riesgos, las vulnerabilidades y los problemas asociados de esta y otras tecnologías relacionadas.

Si bien existen numerosas organizaciones, en el presente trabajo, serán descriptas 2 (dos) de ellas que no tienen un fin comercial y son muy reconocidas, con algunos trabajos de gran relevancia que deberían ser tenidos en cuenta para asegurar el ambiente de *IoT*.

OWASP

Organizaciones como *OWASP* (*Open Web Application Security Project*)[75] generaron distintos proyectos asociados a la problemática *IoT*.

[75] **OWASP** es una comunidad abierta dedicada a permitir a las organizaciones concebir, desarrollar, adquirir, operar y mantener aplicaciones en las que se pueda confiar. Todas las herramientas, documentos, foros y capítulos de OWASP son gratuitos y están abiertos a cualquier persona interesada en mejorar la seguridad de las aplicaciones. https://www.owasp.org/index.php/Main_Page

Ilustración 21 - OWASP
Fuente: https://www.owasp.org/index.php/Main_Page

Proyecto IoT Top Ten

El proyecto *IoT Top Ten* (OWASP, 2019) fue diseñado para colaborar con los fabricantes, desarrolladores y consumidores a comprender mejor los problemas de seguridad asociados con la Internet de las Cosas, y para permitir a los usuarios en cualquier contexto tomar mejores decisiones de seguridad al crear, implementar o evaluar tecnologías de *IoT*.

El proyecto busca definir una estructura para varios subproyectos de *IoT*, como "Áreas de Superficie de Ataque" (descripto más adelante) y "Principales Vulnerabilidades". (descripto, también, más adelante), entre otros.

El mismo fue lanzado en el 2014 y actualizado en 2018.

Tal como el nombre lo indica, selecciona las 10 vulnerabilidades más importantes en las cuales se establecen valores respecto a:

- Explotabilidad
- Prevalencia de la Vulnerabilidad
- Detección de la Vulnerabilidad
- Impacto Técnico

Dichos valores son especificados para diferentes proyectos y se encuentran representados en la siguiente figura:

Agente de Amenaza	Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico	Impacto de Negocio
Específico de la Aplicación	Fácil 3	Difundido 3	Fácil 3	Severo 3	Específico del Negocio
	Promedio 2	Común 2	Promedio 2	Moderado 2	
	Difícil 1	Poco Común 1	Difícil 1	Mínimo 1	

Ilustración 22 - OWASP - Categorías de Evaluación
Fuente: https://github.com/OWASP/Top10/tree/master/2013

Tanto las categorías de Agente de Amenaza como Impacto del Negocio no tienen valores porque pueden ser muy variables al ser dependientes tanto del contexto como del tipo de negocio.

De las 2 versiones descriptas, la más detallada es la del 2014.

Existe un "mapeo" entre ambas debido a que, entre versiones, cambiaron los valores calificados y las posiciones en "ranking" y la clasificación, haciéndose en algunos casos de manera más granular cada análisis.

OWASP IoT Top 10 2014	*OWASP IoT Top 10 2018 Mapping*
I1 Interfaz Web Insegura	I3 Interfaces Inseguras del Ecosistema
I2 Autenticación / Autorización Insuficiente	I1 Contraseñas débiles, adivinables o codificadas
	I3 Interfaces Inseguras del Ecosistema
	I9 Configuraciones Predeterminadas Inseguras
I3 Servicios de Red Inseguros	I2 Servicios de Red Inseguros
I4 Falta de cifrado en el Transporte / Verificación de Integridad	I7 Transferencia o Almacenamiento Inseguro de Datos
I5 Preocupaciones sobre Privacidad	I6 Protección de la Privacidad Insuficiente
I6 Interfaces con la Nube Inseguras	I3 Interfaz Insegura del Ecosistema
I7 Interfaces con dispositivos Móviles Inseguras	I3 Interfaces Inseguras del Ecosistema
I8 Configurabilidad de Seguridad Insuficiente	I9 Configuraciones Predeterminadas Inseguras
I9 Software / Firmware Inseguros	I4 Falta de Mecanismos Seguros de Actualización
	I5 Uso de Componentes Inseguros o Desactualizados
I10 Seguridad Física Insuficiente	I10 Falta de Fortalecimiento Físico

Tabla 2 - OWASP - Proyecto IoT Top 10 - Comparación 2014-2018

Fuente: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=OWASP_IoT_Top_10_2018_Mapping_Project

En la tabla puede observarse que temas asociados a autenticación / autorización eran el segundo riesgo en el 2014 y para el 2018 fueron más detallados y aparecen en distintos niveles en la escala (primero, tercero y noveno).

En la siguiente imagen se representan las diferentes categorías del proyecto OWASP IoT Top 10 de la versión 2018.

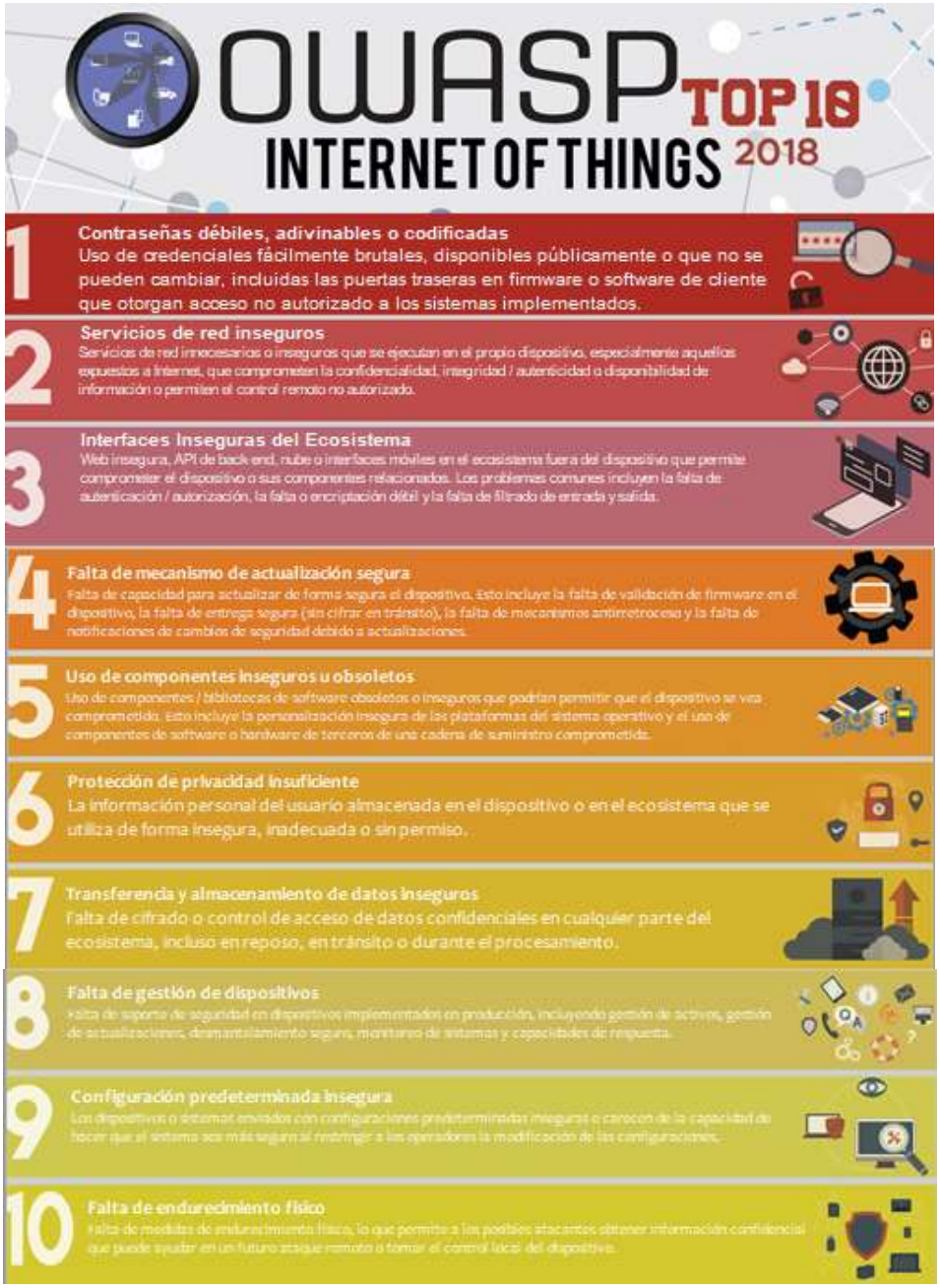


Ilustración 23 - OWASP - Proyecto Top 10 IoT 2018
Fuente: https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf

Focalizándose más en las vulnerabilidades asociadas a la Autorización/Autenticación (2014), graficada en la "ilustración24", puede observarse que observase que cualquier usuario podría tener acceso:

- desde cualquier interfase (web, *mobile*, nube)
- explotando contraseñas débiles o inseguras,
- por el uso de mecanismos de recuperación inseguros,
- con credenciales mal protegidas
- con un control de acceso poco granular.

I2 | Autenticación / Autorización Insuficientes

Agentes de Amenazas	Vectores de Ataque	Debilidad de Seguridad		Impacto Técnico	Impacto del Negocio
Aplicación Específica	Explotabilidad PROMEDIO	Prevalencia COMUN	Detectabilidad FACIL	Impacto SEVERO	Aplicación/Negocio Específico
Considere a cualquiera que tenga acceso a la interfaz web, la interfaz móvil o la interfaz en la nube, incluidos los usuarios internos y externos.	El atacante utiliza mecanismos de recuperación de contraseña débiles, credenciales mal protegidas o falta de control de acceso granular para acceder a una interfaz particular. El ataque podría provenir de usuarios externos o internos.	La autenticación puede no ser suficiente cuando se usan contraseñas débiles o están mal protegidas. La autenticación / autorización insuficiente es frecuente ya que se supone que las interfaces solo estarán expuestas a los usuarios en redes internas y no a usuarios externos en otras redes. Las deficiencias a menudo se encuentran presentes en todas las interfaces. Muchos problemas con la autenticación / autorización son fáciles de descubrir al examinar la interfaz manualmente y también se pueden descubrir a través de pruebas automatizadas.		La autenticación / autorización insuficiente puede provocar la pérdida o corrupción de datos, la falta de responsabilidad o la denegación de acceso y puede llevar a un compromiso total del dispositivo y / o las cuentas de usuario.	Considere el impacto comercial de cuentas de usuario comprometidas y posiblemente dispositivos. Todos los datos pueden ser robados, modificados o eliminados. ¿Podría ser perjudicado su cliente?

Ilustración 24 - OWASP - Proyecto Top 10 IoT 2014 - I2

Fuente: https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

El impacto técnico es calificado como "severo" debido a la posibilidad de acceso directo a los datos.

Estos valores obtenidos llevan a realizarse preguntas del estilo "¿Es suficiente lo que se está haciendo?", tal como se representa en la siguiente ilustración:

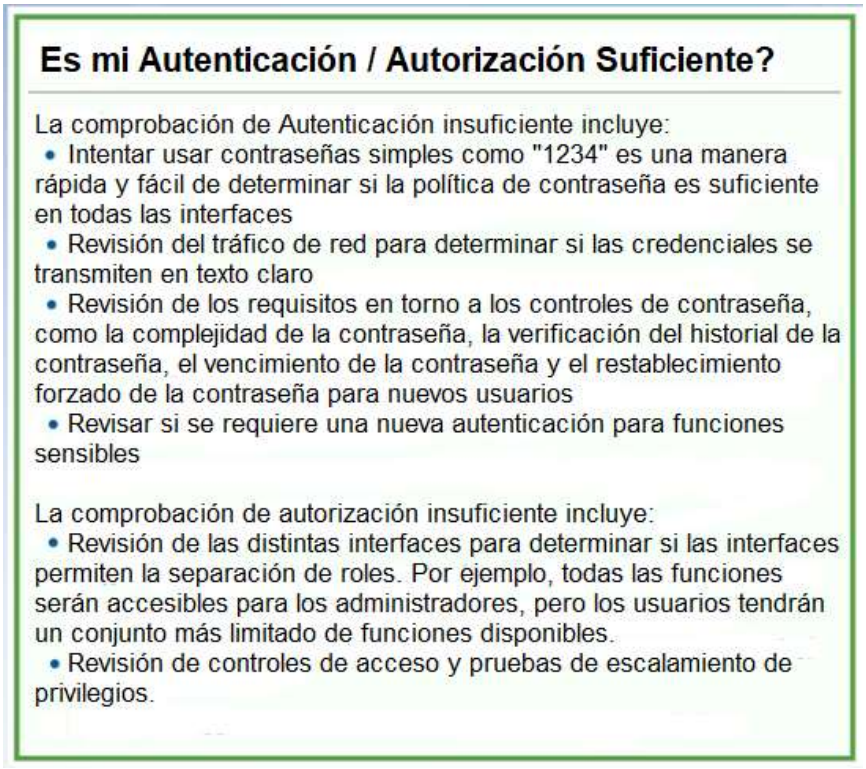


Ilustración 25 - OWASP - Pregunta "¿Es suficiente lo que estoy haciendo?"
Fuente: https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

Del mismo modo, presenta recomendaciones del estilo "¿Qué puede realizarse para mejorar?", como lo representa la siguiente imagen:

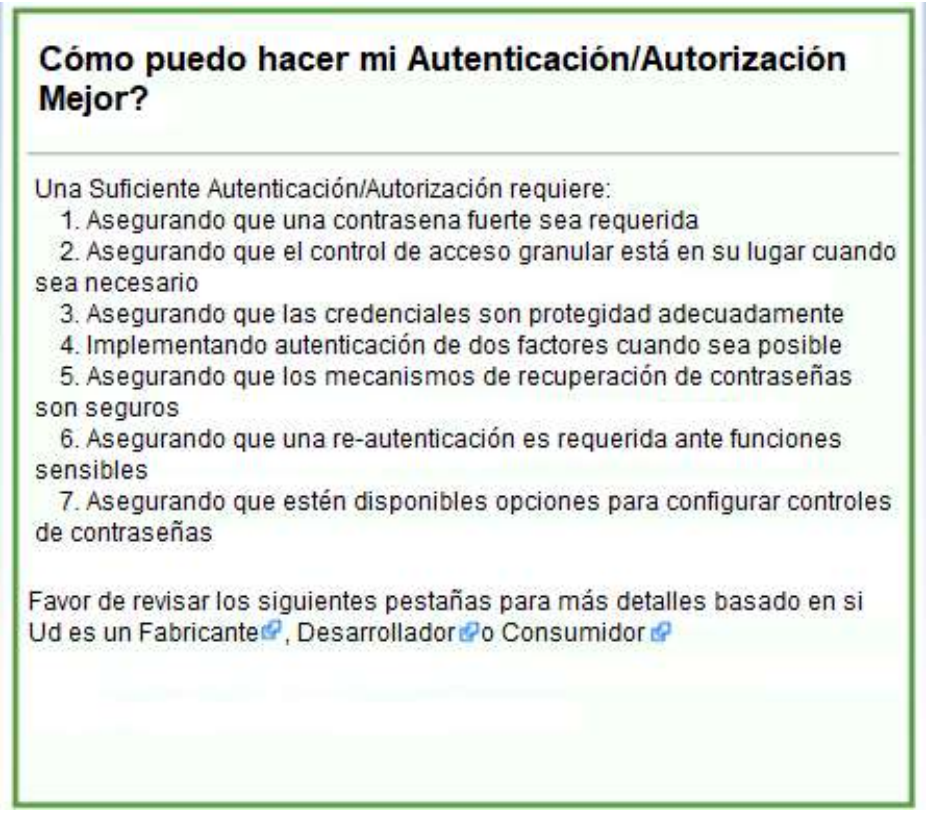


Ilustración 26 - OWASP - Pregunta "¿Qué puede realizarse para mejorar?"
Fuente: https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

Este proyecto es muy interesante para empezar a entender el estado de situación de cualquier proyecto, iniciado o a iniciar.

Proyecto Vulnerabilidades de IoT

El proyecto Vulnerabilidades de *IoT OWASP* (OWASP, 2019) son mencionadas las principales vulnerabilidades de dicho entorno.

Asociadas a cada una de ellas, evidencia las superficies de ataques y ofrece resúmenes de vulnerabilidades relacionadas.

Vulnerabilidad	Superficie de Ataque	Resumen
Enumeración del nombre de usuario	• Interfaz administrativa • Interfaz web del dispositivo • Interfaz de nube • Aplicación móvil	• Capacidad para recopilar un conjunto de nombres de usuario válidos interactuando con el mecanismo de autenticación
Contraseñas débiles	• Interfaz administrativa • Interfaz web del dispositivo • Interfaz de nube • Aplicación móvil	• Posibilidad de configurar las contraseñas de la cuenta en '1234' o '123456' por ejemplo. • Uso de contraseñas predeterminadas preprogramadas
Cierre de cuenta	• Interfaz administrativa	• Posibilidad de continuar

Vulnerabilidad	Superficie de Ataque	Resumen
	• Interfaz web del dispositivo • Interfaz de nube • Aplicación móvil	enviando intentos de autenticación después de 3 a 5 intentos de inicio de sesión fallidos
Servicios no cifrados	• Servicios de red de dispositivos	• Los servicios de red no están correctamente encriptados para evitar las escuchas ilegales o la manipulación por parte de los atacantes
Autenticación de dos factores	• Interfaz administrativa • Interfaz web en la nube • Aplicación móvil	• Falta de mecanismos de autenticación de dos factores, como un token de seguridad o un escáner de huellas dactilares
Cifrado mal implementado	• Servicios de red de dispositivos	• El cifrado se implementa, sin embargo, está mal configurado o no se está actualizando correctamente, por ejemplo, utilizando SSL v2
Actualización enviada sin cifrado	• Mecanismo de actualización	• Las actualizaciones se transmiten a través de la red sin usar TLS o cifrar el propio archivo de actualización
Actualización de la ubicación de escritura	• Mecanismo de actualización	• La ubicación de almacenamiento para los archivos de actualización se puede escribir en todo el mundo y permite que el firmware se modifique y distribuya a todos los usuarios
Negación de servicio	• Servicios de red de dispositivos	• El servicio puede ser atacado de una manera que niegue el servicio a ese servicio o al dispositivo completo
Eliminación de medios de almacenamiento	• Interfaces físicas del dispositivo	• Posibilidad de eliminar físicamente los medios de almacenamiento del dispositivo
No hay mecanismo de actualización manual	• Mecanismo de actualización	• No hay capacidad para forzar manualmente una verificación de actualización para el dispositivo
Falta el mecanismo de actualización	• Mecanismo de actualización	• No se puede actualizar el dispositivo.
Visualización de la versión del firmware y / o Fecha de la última actualización	• Firmware del dispositivo	• La versión actual del firmware no se muestra y / o la fecha de la última actualización no se muestra.
Firmware y extracción de almacenamiento.	• Interfaz JTAG / SWD • Dumping in situ • Interceptando una actualización OTA • Descarga desde la página web	• El firmware contiene mucha información útil, como código fuente y binarios de servicios en ejecución, contraseñas preestablecidas, claves ssh, etc.

Vulnerabilidad	Superficie de Ataque	Resumen
	del fabricante. • eMMC tapping Desoldar el chip SPI Flash / eMMC y leerlo en un adaptador	
Manipulación del flujo de ejecución de código del dispositivo.	• Interfaz JTAG / SWD • Ataques de canal lateral como fallas	• Con la ayuda de un adaptador JTAG y gdb, podemos modificar la ejecución del firmware en el dispositivo y evitar casi todos los controles de seguridad basados en software. • Los ataques de canal lateral también pueden modificar el flujo de ejecución o pueden usarse para filtrar información interesante del dispositivo
Obteniendo acceso a la consola	• Interfaces seriales (SPI / UART)	• Al conectarse a una interfaz serial, obtendremos acceso completo a la consola de un dispositivo • Por lo general, las medidas de seguridad incluyen cargadores de arranque personalizados que evitan que el atacante ingrese al modo de usuario único, pero que también se puede omitir.
Componentes de terceros inseguros	• Software	• Versiones desactualizadas de busybox, openssl, ssh, servidores web, etc.

Tabla 3 - OWASP - Proyecto Vulnerabilidades IoT

Fuente: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities

Este proyecto permite tomar conciencia respecto a los aspectos a evaluar al momento de elegir y/o verificar la tecnología a utilizar.

Queda en evidencia que muchos están asociadas a usuarios, contraseñas y encripción (inexistente o débil implementación).

Si bien no genera un estándar a seguir, permite la obtención un "*checklist*" necesario para el análisis del nivel de "cumplimiento" al momento de la selección o implementación de los distintos componentes.

Proyecto Áreas de Superficie de Ataque de IoT

El Proyecto Áreas de Superficie de Ataque de *IoT OWASP* (OWASP, 2019) se enumeran las Superficies de Ataque que deberían ser conocidas por todos los participantes en la implementación de *IoT*.

- Fabricantes,

- Desarrolladores,
- Investigadores de Seguridad
- Usuarios finales.
- Gobiernos

Superficie de Ataque	Vulnerabilidad
Ecosistema (general)	• Estándares de interoperabilidad • Dato de gobernanza • Fallo en todo el sistema • Riesgos de las partes interesadas individuales • Confianza implícita entre componentes • Seguridad de matriculación • Sistema de desmantelamiento • Procedimientos de acceso perdido

Dispositivo de memoria	• Información delicada
	  • Borrar nombres de usuario
	  • Contraseñas de texto libre
	  • Credenciales de terceros
	  • Claves de cifrado

Interfaces físicas del dispositivo	• Extracción de firmware
	• CLI de usuario
	• Administrador de la CLI
	• Escalada de privilegios
	• Restablecer a estado inseguro
	• Eliminación de medios de almacenamiento
	• Resistencia a la manipulación
	• Puerto de depuración
	  • UART (Serie)
	  • JTAG / SWD
	• ID del dispositivo / Exposición del número de serie

Interfaz web del dispositivo	• Conjunto estándar de vulnerabilidades de aplicaciones web, ver:
	  • OWASP Web Top 10
	  • OWASP ASVS
	  • Guía de pruebas de OWASP
	• Vulnerabilidades de gestión de credenciales:
	  • Enumeración de nombre de usuario
	  • Contraseñas débiles
	  • Cierre de cuenta
	  • Credenciales por defecto conocidas
	Inseguro mecanismo de recuperación de contraseña

Firmware del dispositivo	• Exposición a datos confidenciales (Ver OWASP Top 10 - A6 Exposición a datos sensibles):
	  • Cuentas de puerta trasera
	  • Credenciales codificadas
	  • Claves de cifrado
	  • Cifrado (simétrico, asimétrico)
	  • Información sensible

Superficie de Ataque	Vulnerabilidad
	• Revelación de URL sensible • Muestra la versión del firmware y / o la fecha de la última actualización. • Servicios vulnerables (web, ssh, tftp, etc.) • Verifique las versiones antiguas y posibles ataques (Heartbleed, Shellshock, versiones antiguas de PHP, etc.) • Función relacionada con la seguridad Exposición a la API Posibilidad de rebaja de firmware
Servicios de red de dispositivos	• Divulgación de información • CLI de usuario • CLI administrativo • Inyección • Negación de servicio • Servicios no cifrados • Cifrado mal implementado • Servicios de prueba / desarrollo • Desbordamiento de búfer • UPnP • Servicios UDP vulnerables • DoS • Dispositivo Firmware OTA bloque de actualización • Firmware cargado en canal inseguro (sin TLS) • Ataque repetido • Falta de verificación de la carga útil • Falta de verificación de integridad del mensaje • Vulnerabilidades de gestión de credenciales: • Enumeración de nombre de usuario • Contraseñas débiles • Cierre de cuenta • Credenciales por defecto conocidas • Inseguro mecanismo de recuperación de contraseña
Interfaz administrativa	• Conjunto estándar de vulnerabilidades de aplicaciones web, ver: • OWASP Web Top 10 • OWASP ASVS • Guía de pruebas de OWASP • Vulnerabilidades de gestión de credenciales: • Enumeración de nombre de usuario • Contraseñas débiles • Cierre de cuenta • Credenciales por defecto conocidas • Inseguro mecanismo de recuperación de contraseña • Opciones de seguridad / cifrado • Opciones de registro • Autenticación de dos factores • Compruebe si hay referencias de objetos directos inseguros • Incapacidad para limpiar el dispositivo
Almacenamiento de datos local	• Datos sin cifrar • Datos encriptados con claves descubiertas.

Superficie de Ataque	Vulnerabilidad
	• Falta de controles de integridad de datos • Uso de la misma clave enc / dec estática

Interfaz web en la nube	• Conjunto estándar de vulnerabilidades de aplicaciones web, ver:
	  • OWASP Web Top 10
	  • OWASP ASVS
	  • Guía de pruebas de OWASP
	• Vulnerabilidades de gestión de credenciales:
	  • Enumeración de nombre de usuario
	  • Contraseñas débiles
	  • Cierre de cuenta
	  • Credenciales por defecto conocidas
	  • Inseguro mecanismo de recuperación de contraseña
	• Cifrado de transporte
	• Autenticación de dos factores

API de back-end de terceros	• PII sin cifrar enviado • PII cifrada enviada • Información del dispositivo filtrada • Ubicación filtrada
Mecanismo de actualización	• Actualización enviada sin cifrado • Actualizaciones no firmadas • Actualización de la ubicación de escritura • Verificación de actualización • Autenticación de actualización • Actualización maliciosa • Falta el mecanismo de actualización • No hay mecanismo de actualización manual
Aplicación móvil	• De confianza implícita por dispositivo o nube • Enumeración de nombre de usuario • Cierre de cuenta • Credenciales por defecto conocidas • Contraseñas débiles • Almacenamiento de datos inseguros • Cifrado de transporte • Inseguro mecanismo de recuperación de contraseña • Autenticación de dos factores
API de backend de proveedores	• Confianza inherente a la nube o aplicación móvil. • Autenticación débil • Controles de acceso débiles • Ataques de inyección • Servicios ocultos
Comunicación del ecosistema	• Controles de salud • Latidos del corazón • Comandos del ecosistema • Desprovisionamiento • Envío de actualizaciones
Tráfico de red	• LAN • LAN a Internet

Superficie de Ataque	Vulnerabilidad
	• Corto alcance • No estándar • Inalámbrico (WiFi, Z-wave, XBee, Zigbee, Bluetooth, LoRA) • Protocolo fuzzing
Autorización/Autenticación	• Autenticación / Autorización de valores relacionados (clave de sesión, token, cookie, etc.) divulgación • Reutilización de clave de sesión, token, etc. • Dispositivo a autenticación de dispositivo • Dispositivo de autenticación de aplicaciones móviles • Dispositivo para la autenticación del sistema en la nube • Aplicación móvil para la autenticación del sistema de nube. • Autenticación de la aplicación web a la nube. • Falta de autenticación dinámica
Privacidad	• Revelación de datos de usuario • Revelación de la ubicación del usuario / dispositivo • Privacidad diferencial
Hardware (Sensores)	• Sensación de la manipulación del entorno • Manipulación (físicamente) • Daño (Físico)

Tabla 4 - OWASP - Áreas de Superficie de Ataque de IoT

Fuente: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Attack_Surface_Areas

Este proyecto permite estudiar los distintos flancos que deberían ser analizados y cubiertos al momento de la implementación.

Es una lista bastante extensa, que permite realizar un análisis profundo de todo el ecosistema.

Mitre – CVE (Common Vulnerabilities and Exposures

Organizaciones como Mitre[76] administran un sitio denominado *CVE (Common Vulnerabilities and Exposures)* (Mitre, 2019), representada por la "ilustración 27", que tiene una base de datos de vulnerabilidades, denominada *NVD (National Vulnerability Database)*, junto con el *NIST*[77], reproducido en la "ilustración 28", permitiendo documentar las vulnerabilidades encontradas en los distintos sistemas y tecnologías.

[76] **Mitre**: Empresa dedicada a la seguridad. Trabaja con tema de Defensa e inteligencia, aviación, Seguridad Nacional, Salud y Ciberseguridad https://www.mitre.org/

[77] **NIST** por sus siglas en inglés *National Institute of Standards and Technology*. Instituto Nacional de Estándares y Tecnología. El progreso e innovación tecnológica de Estados Unidos dependen de las habilidades del *NIST*, especialmente si hablamos de cuatro áreas: biotecnología, nanotecnología, tecnologías de la información y fabricación avanzada

Ilustración 27 - Mitre - Common Vulnerabilities and Exposures
Fuente: https://cve.mitre.org/index.html

Ilustración 28 - NIST National Vulnerabolity Database
Fuente: https://nvd.nist.gov/

Dicha base almacena la siguiente información:

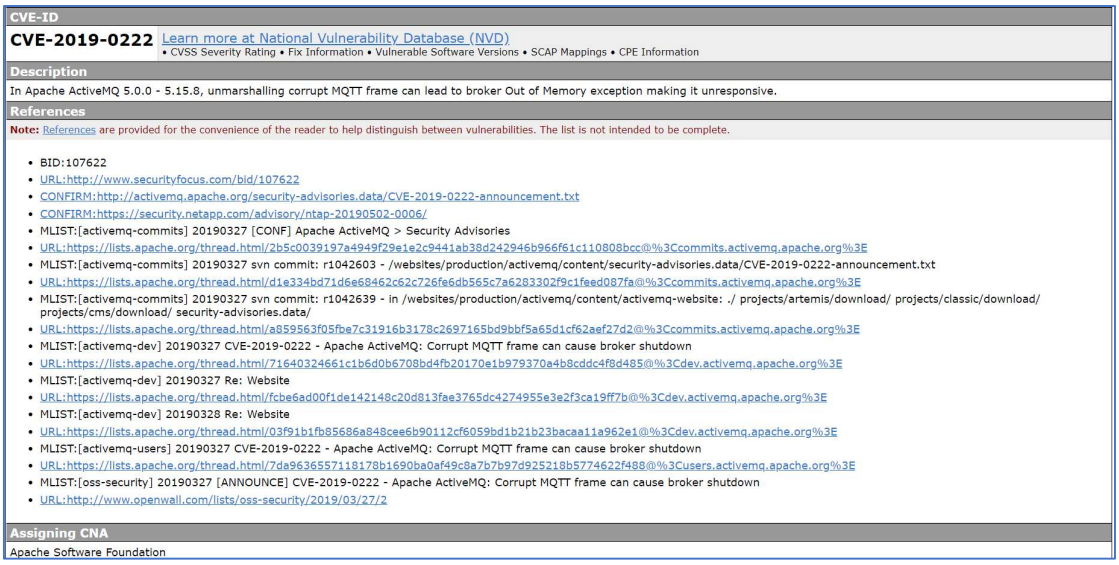
- ***ID***: formado por el año y un número secuencial.
- ***Descripción***: descripción de la vulnerabilidad.
- ***Referencias***: en las cuales se encuentran adjuntados los documentos sobre quienes las encontraron y las posibles soluciones.
- ***Fecha de Creación del registro en la base de datos***: fecha de creación dentro de la NVD.

Este sitio permite realizar búsquedas por tecnología, fabricante y distintas palabras clave de manera de obtener la información de posibles vulnerabilidades en la tecnología *IoT*, y conocer cómo fueron encontradas, si las mismas tienen ya solución parcial y/o definitiva por parte del fabricante.

Ejemplo *MQTT*:

- **CVE-2019-0222**: Un frame corrupto especialmente diseñado para *MQTT* ejecutando en Apache ActiveMQ 5.0.0 5.15.8, puede conducir a que el *Broker* tenga una

excepción del tipo "*Out of Memory*" y no responda, siendo susceptible a fallas del tipo de "Denegación de Servicios", representada por la siguiente imagen:



CVE-ID

CVE-2019-0222 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

In Apache ActiveMQ 5.0.0 - 5.15.8, unmarshalling corrupt MQTT frame can lead to broker Out of Memory exception making it unresponsive.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

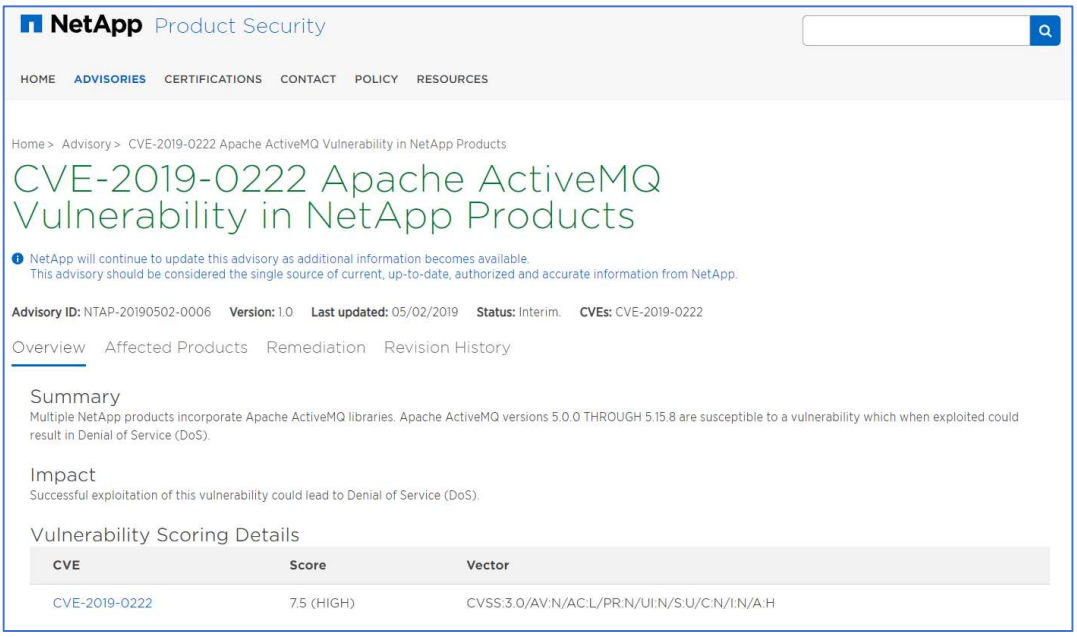
- BID:107622
- URL:http://www.securityfocus.com/bid/107622
- CONFIRM:http://activemq.apache.org/security-advisories.data/CVE-2019-0222-announcement.txt
- CONFIRM:https://security.netapp.com/advisory/ntap-20190502-0006/
- MLIST:[activemq-commits] 20190327 [CONF] Apache ActiveMQ > Security Advisories
- URL:https://lists.apache.org/thread.html/2b5c0039197a4949f29e1e2c9441ab38d242946b966f61c110808bcc@%3Ccommits.activemq.apache.org%3E
- MLIST:[activemq-commits] 20190327 svn commit: r1042603 - /websites/production/activemq/content/security-advisories.data/CVE-2019-0222-announcement.txt
- URL:https://lists.apache.org/thread.html/d1e334bd71d6e68462c62c726fe6db565c7a6283302f9c1feed087fa@%3Ccommits.activemq.apache.org%3E
- MLIST:[activemq-commits] 20190327 svn commit: r1042639 - in /websites/production/activemq/content/activemq-website: ./ projects/artemis/download/ projects/classic/download/ projects/cms/download/ security-advisories.data/
- URL:https://lists.apache.org/thread.html/a859563f05fbe7c31916b3178c2697165bd9bbf5a65d1cf62aef27d2@%3Ccommits.activemq.apache.org%3E
- MLIST:[activemq-dev] 20190327 CVE-2019-0222 - Apache ActiveMQ: Corrupt MQTT frame can cause broker shutdown
- URL:https://lists.apache.org/thread.html/71640324661c1b6d0b6708bd4fb20170e1b979370a4b8cddc4f8d485@%3Cdev.activemq.apache.org%3E
- MLIST:[activemq-dev] 20190327 Re: Website
- URL:https://lists.apache.org/thread.html/fcbe6ad00f1de142148c20d813fae3765dc4274955e3e2f3ca19ff7b@%3Cdev.activemq.apache.org%3E
- MLIST:[activemq-dev] 20190328 Re: Website
- URL:https://lists.apache.org/thread.html/03f91b1fb85686a848cee6b90112cf6059bd1b21b23bacaa11a962e1@%3Cdev.activemq.apache.org%3E
- MLIST:[activemq-users] 20190327 CVE-2019-0222 - Apache ActiveMQ: Corrupt MQTT frame can cause broker shutdown
- URL:https://lists.apache.org/thread.html/7da963655711817 8b1690ba0af49c8a7b7b97d925218b5774622f488@%3Cusers.activemq.apache.org%3E
- MLIST:[oss-security] 20190327 [ANNOUNCE] CVE-2019-0222 - Apache ActiveMQ: Corrupt MQTT frame can cause broker shutdown
- URL:http://www.openwall.com/lists/oss-security/2019/03/27/2

Assigning CNA

Apache Software Foundation

Ilustración 29 - Ejemplo Vulnerabilidad Mitre – CVE-2019-0222
Fuente: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0222

Dentro de las referencias puede encontrarse al fabricante y toda la documentación asociada, como la representada en la siguiente ilustración:



NetApp Product Security

HOME ADVISORIES CERTIFICATIONS CONTACT POLICY RESOURCES

Home > Advisory > CVE-2019-0222 Apache ActiveMQ Vulnerability in NetApp Products

CVE-2019-0222 Apache ActiveMQ Vulnerability in NetApp Products

NetApp will continue to update this advisory as additional information becomes available.
This advisory should be considered the single source of current, up-to-date, authorized and accurate information from NetApp.

Advisory ID: NTAP-20190502-0006 **Version:** 1.0 **Last updated:** 05/02/2019 **Status:** Interim. **CVEs:** CVE-2019-0222

Overview Affected Products Remediation Revision History

Summary

Multiple NetApp products incorporate Apache ActiveMQ libraries. Apache ActiveMQ versions 5.0.0 THROUGH 5.15.8 are susceptible to a vulnerability which when exploited could result in Denial of Service (DoS).

Impact

Successful exploitation of this vulnerability could lead to Denial of Service (DoS).

Vulnerability Scoring Details

CVE	Score	Vector
CVE-2019-0222	7.5 (HIGH)	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Ilustración 30 - Referencias Vulnerabilidad Mitre – CVE-2019-0222
Fuente: https://security.netapp.com/advisory/ntap-20190502-0006/

Como puede observarse en la imagen, se encuentra detallada información como descripciones, productos afectados, remediación y un historial de la falla.

Del mismo modo podrían ser buscados protocolos, fabricantes, productos u otras palabras claves para realizar la búsqueda en dicha base.

La ventaja y, desventaja al mismo tiempo, es que en el caso de que tanto los investigadores/desarrolladores/implementadores como los atacantes conozcan datos de la instalación, podrán conocer también sus vulnerabilidades y actuar en consecuencias, tanto para bien como para mal.

Conceptos sobre autenticación propiamente dicha

Mas allá de los proyectos descriptos anteriormente, hay temas específicos sobre autenticación que deben ser analizados de manera más detallada.

Gestión de la Identidad y acceso Para IoT

Antes de implementar una red de dispositivos *IoT*, sería necesario establecer criterios para realizar una buena gestión de las identidades de los equipos.

Esto es debido a que esta tecnología presenta nuevos desafíos constantemente. Para citar un ejemplo sobre la administración, los equipos no necesariamente deben ser de nuestra propiedad, pueden ser alquilados, como pasa con los servicios de *AWS*[78] de Amazon.

Por dicho motivo, el sistema de Gestión de Identidades y Acceso (*IAM* en inglés, proveniente de *Identity and Access Management*) debería permitir este comportamiento dinámico para poder permitir la aceptación o el rechazo rápidos para compartir la información.

Ciclo de Vida de la Identidad

Es de mucha utilidad administrar correctamente el ciclo de vida de identidad de los dispositivos. El mismo comienza cuando se realizan las convenciones de nomenclatura de los dispositivos y termina al momento de darlo de baja del sistema.

Este procedimiento de ciclo de vida debe ser llevado a cabo para todo dispositivo que se adquieran, configuren y conecten a la red, analizando de manera concienzuda las distintas categorías a las cuales pueden pertenecer ahora o en el futuro. El mismo es representado por la siguiente ilustración:

[78] AWS Servicios de IoT para soluciones comerciales, industriales y para consumidores de la empresa Amazon https://aws.amazon.com/es/iot/?hp=tile&tile=solutions

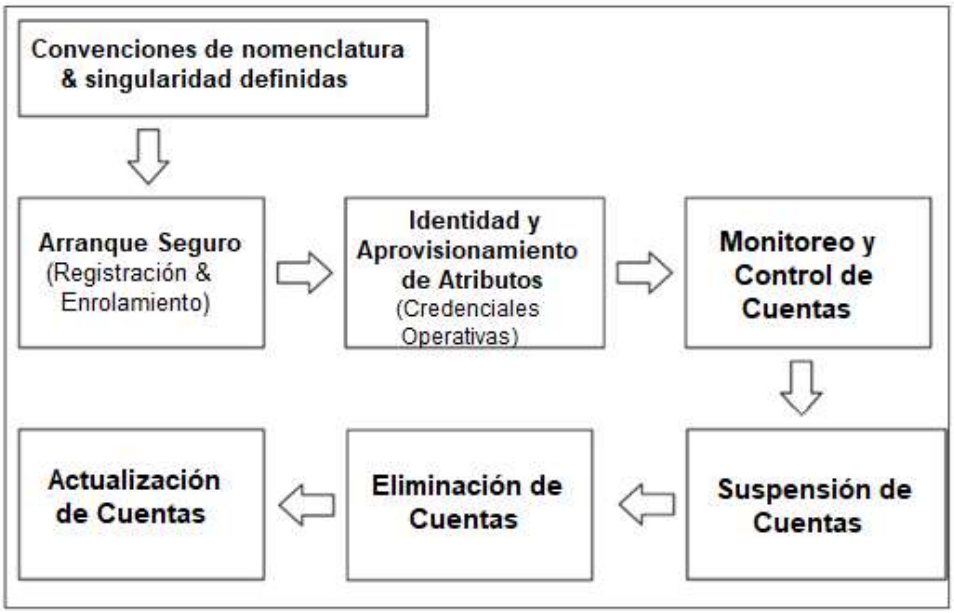


Ilustración 31 - Ciclo de Vida de la Identidad
Fuente: www.allitebooks.org/practical-internet-of-things-security/

Convención de nombres/ Identificadores

Al comienzo de este ciclo es importante establecer el espacio de nombres de identidades adecuado para la cantidad de dispositivos que hagan falta conectar, previendo un crecimiento

Arranque seguro

Otro de los temas que se deben tener en cuenta son los arranques seguros de los diferentes dispositivos. Uno de los peores casos para la seguridad en una red de *IoT* es cuando en la red existe un sin número de identidades falsas que terminan convirtiéndose en suplantaciones de identidad, robo de información privada, falsificación o caos.

El proceso de arranque el comienzo del aprovisionamiento de una identidad de confianza para un dispositivo. El mismo puede comenzar con el propio fabricante (con un chip) y ser concluido cuando el usuario lo recibe. Entre ellos podemos nombrar los números de serie e identificadores únicos establecidos en memorias del tipo *ROM*[79].

Este proceso debe adaptarse al entorno de amenazas que tiene el dispositivo, sus capacidades y el entorno de red. Ante mayor riesgo, más estricto y completo deberá ser el proceso de arranque.

[79] **Memorias ROM**: del inglés *Read Only Memory*. Memoria de sólo lectura.

Acceso local

Con fines administrativos, muchas veces será necesario ingresar al dispositivo de manera local. Hay que tener en cuenta cual sería la solución a implementar para el acceso, teniendo presente:

- si hay grandes distancias entre dispositivos,
- los diferentes dispositivos (sensores, etc.)
- las posibilidades de una administración centralizada de las contraseñas.

Actualización de Cuentas

Una buena práctica, altamente difundida, es la rotación de las credenciales (certificados, contraseñas, claves).

Muchas veces, impedimentos logísticos han sido un obstáculo para acortar la vida de las mismas y para gestionar un creciente número de credenciales.

Si bien la rápida rotación reduce algunos tipos de ataques, el proceso de realizar dichos cambios puede ser lento y costo.

Suspensión de Cuentas

Tal como ocurre con las cuentas de los usuarios "personas", sería recomendable poder suspender las cuentas de los dispositivos de *IoT* por si fuera necesario algún tipo de análisis forense posterior.

Desactivación/eliminación de cuentas/credenciales

La eliminación definitiva de las cuentas utilizadas por los dispositivos y los servicios que interactúan colaboran de una manera muy importante para combatir los posibles ataques en los cuales intentan obtener accesos cuando los dispositivos están ya fuera de servicio.

CAPITULO IV – Solución

(Página en blanco)

Introducción

Han quedado en evidencia los riesgos y algunas técnicas para reducirlos. Han sido mencionadas algunas actividades a tener en cuenta para poder mejorar la situación actual sobre la seguridad de la tecnología *IoT*, basadas en recomendaciones generales y las vulnerabilidades descubiertas sobre las instalaciones ya realizadas y/o a lanzadas y/o a ser lanzadas al mercado.

Sería más conveniente poder generar todos los pasos necesarios para el aseguramiento, mencionados anteriormente, previo a la salida "a la calle" de los productos y /o dispositivos.

Permitiendo la planificación anticipada de toda la actividad y la organización de las necesidades de uso que los usuarios finales puedan tener sin restarle importancia a los aspectos de seguridad.

La propuesta del presente trabajo sería que, como en otras industrias y/o procesos – que pueden o no tener aspectos tecnológicos – se establezca un estándar para trabajar.

Ejemplos exitosos de este tipo de esta metodología han sido:

- Protocolos de transmisión de datos, ejemplo *TCP/IP*
- Convenios sobre nombres de países para la gestión de las páginas web
- Dispositivos electroópticos como el DVD
- Normas técnicas sobre celulares, etc.
- Recomendaciones de Seguridad de la Información: familia ISO 27000

En el caso del estándar para *IoT*, deberían ser analizados

- Todas las superficies de ataque
- Vulnerabilidades descriptas y otras que, por motivos de alcance, quedaron fuera del presente trabajo.

Cuando una tecnología "pierde la confianza" de los usuarios actuales o futuros, en este caso por parte de algún ataque, no sólo pierde la empresa afectada. Dicha pérdida alcanza a todos los participantes de la implementación:

- usuarios finales,
- proveedores,
- fabricantes

- gobierno.

Estas pérdidas pueden no llegar a ser monetizables o puede ser muy difícil obtener un único valor. Pero serán, certeramente, cuantiosas.

Por dichos motivos, surge la necesidad de que todos los actores mencionados deberían exigir y, a su vez, colaborar para el establecimiento de estándares que valoren más la seguridad que la cantidad de dispositivos a vender o la rapidez con la cual se llega a un mercado.

Deben ser definidas las pautas de seguridad pertinentes, respetando:

- la confidencialidad
- la integridad
- disponibilidad

de los datos, procesos y personas participantes.

En este proceso, tal como ocurre con otros estándares relacionados o basados en procesos de gestión y/o calidad total, se debería plantear el círculo virtuoso de "Planificar, Hacer, Verificar y Actuar" (*Plan-Do-Check-Act*) (Ingrande, 2018), representado en la "ilustración 32", para consensuar y organizar los trabajos, ciclos de vida de los productos, criterios de obsolescencia, protección, contramedidas, etc.

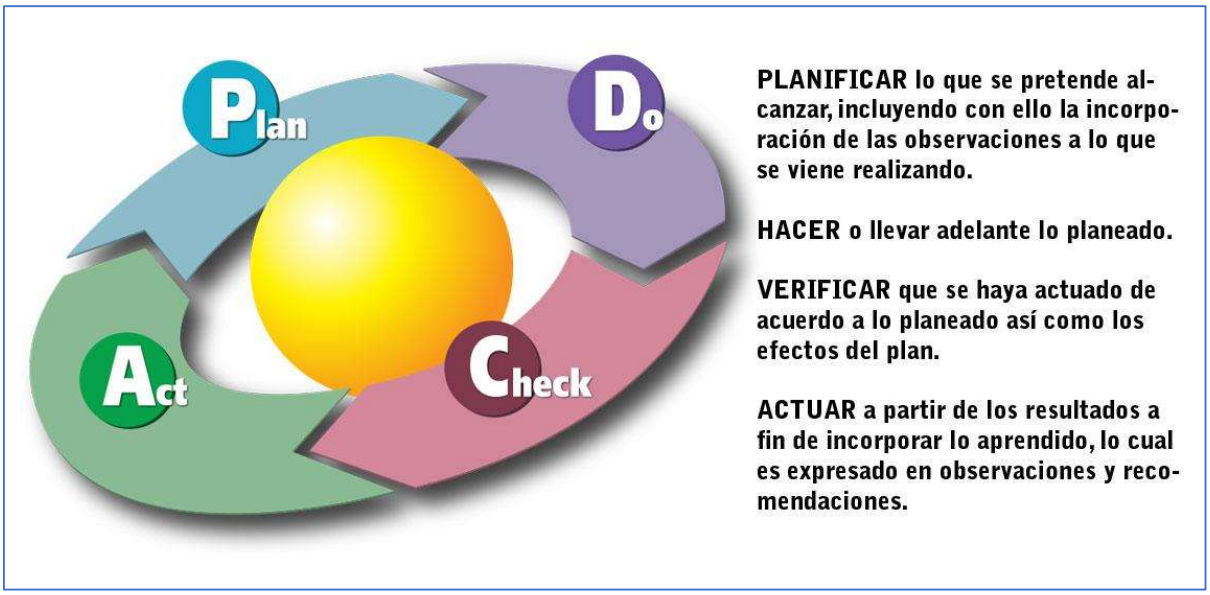


Ilustración 32 - Ciclo Planificar, Hacer, Verificar y Actuar
Fuente: https://es.wikipedia.org/wiki/Ciclo_de_Deming#/media/Archivo:PDCA_Cycle.svg

Estándares por generar

Dentro de los estándares a generar, deben verificarse que se tengan en cuentas algunos conceptos básicos de seguridad, tal vez, agrupados en diferentes temas.

En el caso de este trabajo, se han clasificado en 2 diferentes ramas: Autenticación y Otros.

Autenticación

Temas relacionados con claves / contraseñas y o credenciales:

- Evitar contraseñas débiles / conocidas / calculables / atacables por medio de diccionarios / o la carencia de ellas por medio de las recomendaciones ya vistas o tomado los estándares de seguridad conocidos.
- Verificar que todas las contraseñas posean un nivel de complejidad aceptable.
- En el caso de necesitar mecanismos de recuperación de contraseñas, verificar que estos sean seguros, garantizando que el solicitante sea el correcto.
- En caso de utilizar funciones/operaciones que accedan a datos sensibles, asegurar pasos de re-autenticación o confirmación para la realización de la operación.
- Eliminar "ventanas de tiempo vulnerables" en protocolos de intercambio o enrolamiento.
- Implementar mecanismos para evitar la enumeración de cuentas
- Verificar mecanismos de bloqueos de cuentas
- Limitar, o directamente eliminar las opciones que permitan poner volver a las contraseñas por defecto (*factory reset*)[80]
- Verificar que las credenciales no sean expuestas dentro del tráfico de red.
- No descuidar los aspectos relacionados con el almacenamiento

Otros

En este apartado, son agrupados y detallados ítems relacionados a almacenamiento, acceso físico y actualizaciones.

[80] ***Factory Reset***: Acción de volver a los valores configurados de fábrica, también llamados "por defecto".

Temas relacionados con el almacenamiento:

- Verificar la manera en la cual es almacenada información dentro del dispositivo (claves de encripción, credenciales y datos sensibles.). Ubicación y algoritmo de cifrado (si fuese necesario).
- Estudiar mecanismos de "*anti-tampering*"[81] tomando en cuenta la posibilidad destrucción de la información o el propio dispositivo, siendo cuidadoso de no genera una pérdida innecesaria de datos, del equipo y/o una denegación de servicio.

Temas relacionados con el acceso físico

- Analizar conceptos de "cuarentena" para aquellos dispositivos que hayan sido accedidos de manera "irregular".
- Encriptar datos de los medios de almacenamiento removibles.
- Limitar los accesos vía puertos (USB, otros) a datos (sensibles o no)
- Implementar mecanismos de resiliencia

Temas de Actualizaciones

- Mejorar la autenticidad de las actualizaciones.
- Verificar la encripción de las actualizaciones.
- Controlar pasar de un estado seguro a otro[82]
- Verificar que no se permitan "*downgrade*"[83] de versiones.
- Poder conocer el tiempo mínimo en el cual el fabricante puede poner a disposición las actualizaciones de seguridad
- Conocer puntos de contacto con los fabricantes/proveedores para divulgación de vulnerabilidades y sus tiempos de solución y mecanismos de reparación

Procedimientos

Producto del análisis y la puesta en práctica los temas mencionados, sería posible elevar la seguridad desde el inicio del proceso de despliegue de la tecnología y se obtendrá toda la información necesaria para generar los procedimientos de gestión necesarios, desde los más técnicos hasta las recomendaciones para usuarios finales.

[81] **Anti-tampering**: Técnicas para evitar la alteración o manipulación de objetos

[82] Si un objeto era considerado seguro, luego de la actualización, debería poder seguir siéndolo.

[83] "**Downgrade**": Es un término normalmente utilizado en el ámbito del software. Significa devolver el software a una antigua versión. Podría ser de inferior calidad o seguridad

CAPITULO V – Validación

(Página en blanco)

Durante la búsqueda y análisis del material para la realización del presente trabajo se hicieron públicas noticias provenientes del Reino Unido que permiten validar las propuestas realizadas.

La primera de ellas, relacionadas con un Centro dedicado al desarrollo de estándares de ciberseguridad en *IoT*.

La otra, vinculada con la creación de leyes de protección contra ataques cibernéticos a los dispositivos involucrados en esta tecnología.

Centro dedicado al desarrollo de estándares de ciberseguridad en IoT

Reino Unido creó, a principio de 2019, un Centro de Excelencia (IoT News, 2019) denominado *PETRAS National Centre of Excellence for IoT Systems Cybersecurity*. *PETRAS*[84] son siglas de *Privacy, Ethics, Trust, Reliability, Acceptability, and Security* (Privacidad, Ética, Confianza, Confiabilidad, Aceptabilidad y Seguridad), representado en la "ilustración 33".

El mismo se dedicará al desarrollo y promoción de estándares de ciberseguridad de *IoT*.

Esto permite poner al Reino Unido entre los primeros en realizar este tipo de actividades en este campo.

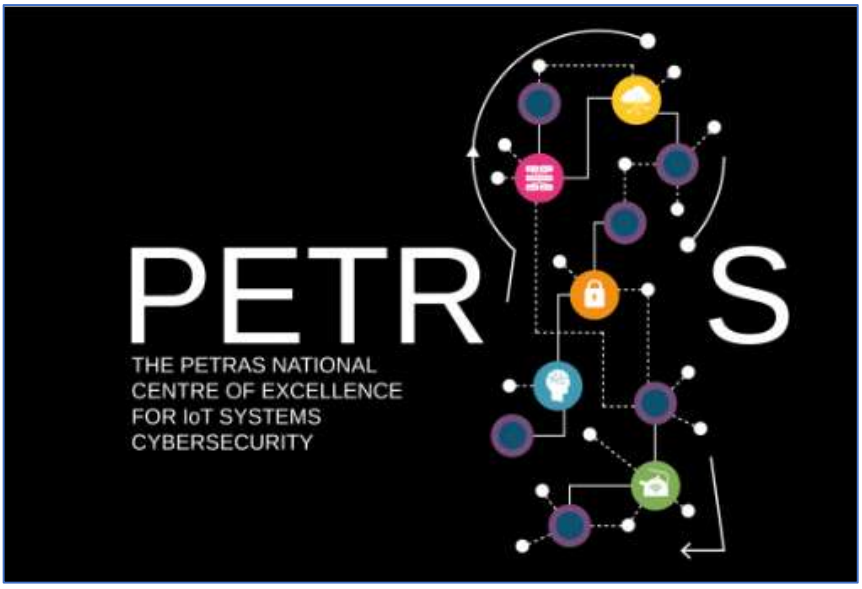


Ilustración 33 - Logo Petras
Fuente: https://petras-iot.org/

[84] "*The PETRAS National Centre of Excellence*" https://www.petrashub.org/

La organización *PETRAS* fue fundada en 2016 y está compuesta por 11 universidades (*Cardiff University, Imperial College London, Lancaster University, Newcastle University, The University of Edinburgh, The University of Warwick, University of Bristol, University of Nottingham, University of Oxford, University of Southampton*, *University of Surrey*) y 110 participantes pertenecientes a industria y gobierno (Intel, Cisco, Telefónica, Agencia Nacional del Crimen – *NCA*[85] – entre otros).

Entre sus temas y áreas de trabajo se encuentran:

- Autenticación y control de acceso con múltiples dispositivos IoT, de *"Authentication and Access Control with Multiple IoT Devices" (AACIoT)*
- Plataforma de estándares multidisciplinarios de IoT, de *"IoT Multi-disciplinary Standards Platform" (IoTMSP)*
- Confianza y privacidad como principios de diseño para infraestructuras de IoT, de *"Trust and Privacy as Design Principles for IoT Infrastructures" (DePrIoT)*
- Modelo de evaluación de impacto para el IoT, *de "Impact Assessment Model for the IoT" (IAM)*
- Ciberseguridad de IoT en Infraestructura Crítica Nacional, de *"Cyber Security of IoT in Critical National Infrastructure" (IoTinCNI)*
- Valor de los datos personales en IoT, de *"Value of Personal Data in IoT" (VPD)*
- Desarrollo de un índice de seguridad del consumidor para dispositivos IoT del consumidor, de *"Developing a Consumer Security Index for Consumer IoT devices" (CSI)*
- Obediencia de las Cosas en espacios privados, de *"Respectful Things in Private Spaces" (ReTiPS)*
- Código de prácticas de la red de área local, de *"Home Area Network Code of Practice" (HANCODE)*
- Privacidad y confianza en automóviles autónomos conectados y transporte inteligente, de *"Privacy and Trust in Connected Autonomous Cars and Smart Transport" (PEIESI)*

[85] **NCA**: *UK National Crime Agency*. Agencia Nacional contra el Crimen del Reino Unido.

- Identificación de vectores de ataque para la intrusión en la red para determinar el impacto en las superficies de amenaza (dependientes de IoT), de *"Identifying Attack Vectors for Network Intrusion to Determine Impact Across Threat Surfaces" (IoT-Depends)*
- Evaluación de riesgos de seguridad de entornos IoT con modelos de gráficos de ataque, de *"Security Risk Assessment of IoT Environments with Attack Graph Models" (SECRIS)*
- Evaluación de los requisitos de los sistemas IoT para las aplicaciones de seguimiento, de *"Evaluation of IoT Systems' Requirements for Tracking Applications" (Things d'Art)*
- Auditoría de demostradores de transporte y movilidad, de *"Transport and Mobility Demonstrator Audit" (TMDA)*
- Desarrollo de un Índice de Seguridad del Consumidor para dispositivos domésticos IoT Plus, de *"Developing a Consumer Security Index for Domestic IoT devices Plus" (CSI+)*
- Hacer visible lo invisible: pantallas y sensores IoT seguros y confiables para entornos urbanos en CityVerve[86], de *"Making the Invisible Visible – Secure, Trustworthy IoT Displays and Sensors for Urban Environments in CityVerve" (IDice)*
- Seguridad en IoT para el Cuidado de la Salud, de *"IoT Security for Health Care" (SeNTH +)*
- Política nacional e internacional para ciberseguridad de infraestructura crítica, de *"National and International Policy for Critical Infrastructure Cybersecurity" (NiPC)*
- Asegurando el Valor de la Medición Inteligente, de *"Securing the Value of Smart Metering" (SeMIoT)*
- IoT bajo Control, de *"IoT in Control"*

[86] **CityVerve**: Demostrador de SmartCity de Manchester. Proyecto de ciudad inteligente realizado para explorar cómo se puede utilizar la tecnología para mejorar la vida de todos los ciudadanos, que permite recolectar y compartir información, desde la atención médica y el transporte hasta la cultura y el medio ambiente. (https://cityverve.org.uk/)

Leyes para protección contra ataques cibernéticos a los dispositivos de IoT

El gobierno del Reino Unido ha anunciado planes para la creación de nuevas leyes que tienen como objetivo proteger los dispositivos de *IoT* de los ataques cibernéticos. (IoT News, 2019)

La ministra Margot James, encargada del Ministerio de Asuntos Digitales, Cultura, Medios y Deporte reveló medidas en un intento por frenar el enorme crecimiento en ataques dirigidos a dispositivos conectados, estableciendo un primer paso para asegurarnos de que los productos tengan características de seguridad integradas desde la etapa de diseño. (Government of UK, Department for Digital, Culture, Media & Sport, 2019)

Estas nuevas propuestas ayudarán a mejorar la seguridad de los dispositivos conectados a Internet y es un concepto de avanzada que pone al Reino Unido como pionero en el tema.

Las leyes también incluirán las pautas de "Asegurar por diseño" exigiendo las siguientes características:

- Las contraseñas de los dispositivos *IoT* deberán ser únicas y no deberían poder ser restablecidas a una configuración predeterminada de fábrica.
- Los fabricantes de productos de *IoT* deberán proporcionar un punto de contacto público como parte de una política de divulgación de vulnerabilidades.
- Los fabricantes deberán declarar explícitamente el tiempo mínimo durante el cual el dispositivo recibirá actualizaciones de seguridad a través de una política de fin de vida útil.

Gigantes de la tecnología global – entre los cuales pueden mencionarse a Amazon, Philips, Panasonic y Samsung – participaron en la “mesa redonda” propuesta por la ministra, comprometiéndose a garantizar que sus productos cumplan con los requisitos de seguridad propuestos.

No cabe duda de que este tipo de iniciativas generarán un “círculo virtuoso”, o al menos ayudarán, a favor de la tecnología y de todos los usuarios en lo que respecta a la seguridad.

Primeros trabajos

Producto del trabajo en conjunto de Gobierno de Reino Unido con el organismo *PETRAS*, surgieron documentos, base para el aseguramiento de *IoT*. Los mismos se encuentran alojados en el sitio del Ministerio antes mencionado, como una colección denominada "Seguro por Diseño"

Ente ellos se destacan:

"*Code of Practice for Consumer IoT Security*"

"Código de Prácticas de Seguridad del Consumidor en relación con el Internet de las Cosas", representado en la "ilustración 34"

- Presenta las prácticas recomendadas destinadas a fabricantes, proveedores de servicios de *IoT*, desarrolladores de aplicaciones móviles y vendedores minoristas
- Aplicable a productos que están conectados a internet o a redes domésticas y/o servicios asociados, entre los que se destacan:
    - Juguetes de niños y monitores infantiles conectados a Internet,
    - Productos de seguridad con conexión a Internet, como detectores de humo y cerraduras de puertas,
    - Televisores, altavoces y cámaras inteligentes
    - Accesorios inteligentes "*wereables"* para monitorear la salud,
    - Sistemas de alarma y automatización del hogar con conexión a Internet,
    - Electrodomésticos con conexión a Internet (por ejemplo, lavarropas, heladeras),
    - Asistentes inteligentes para el hogar
- Presenta 13 Normas:
    - 1) No utilizar contraseñas predeterminadas
    - 2) Implementar una política de divulgación de vulnerabilidades
    - 3) Mantener el software actualizado
    - 4) Guardar las credenciales y los datos confidenciales de forma segura
    - 5) Comunicarse de forma segura
    - 6) Reducir las superficies expuestas a ataques
    - 7) Garantizar la integridad del software
    - 8) Asegurar que los datos personales estén protegidos

    - 9) Hacer que los sistemas sean flexibles en casos de desconexión o cortes de energía
    - 10) Supervisar los datos de telemetría del sistema
    - 11) Facilitar la eliminación de datos personales por parte de los consumidores
    - 12) Hacer que la instalación y el mantenimiento de los dispositivos sean sencillos
    - 13) Validar los datos de entrada
- Puesto a disposición en Octubre de 2018
- Tiene versiones en diferentes idiomas y regiones y son previstas revisiones, al menos cada 2 años

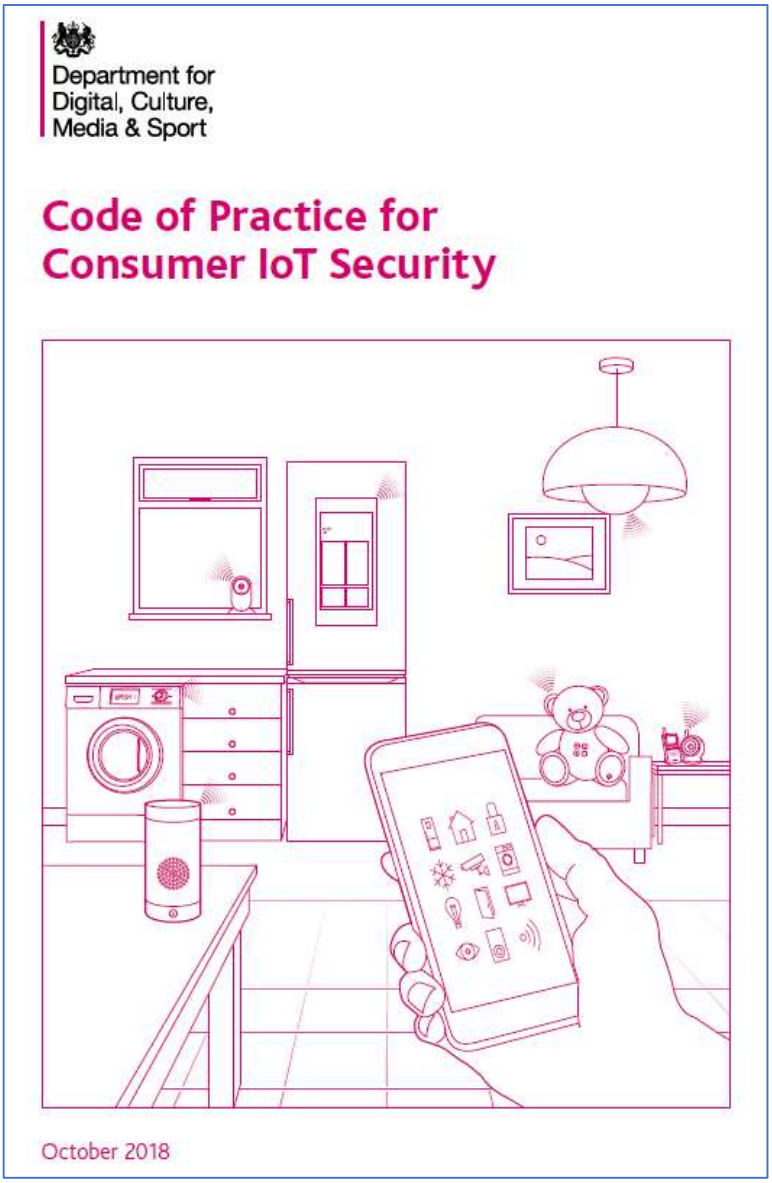


Ilustración 34 – "Code of Practice for Consumer IoT Security"
Fuente:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

"Mapping of IoT security recommendations, guidance and standards"

"Mapeo de Recomendaciones de Seguridad de *IoT*, Guías y Estándares"

- Presenta las Relaciones entre el "Código de Prácticas de Seguridad del Consumidor en relación con el Internet de las Cosas" contra los estándares publicados, recomendaciones y orientación sobre seguridad y privacidad de *IoT* de todo el mundo.

- Si bien no es exhaustivo, comprende una revisión de alrededor de 100 documentos de casi 50 organizaciones, representando una de las mayores colecciones de documentos orientados al tema hasta la fecha.
- El propósito del mapeo es servir como referencia y herramienta para los usuarios del Código de Prácticas. Los fabricantes y otras organizaciones ya están implementando una gama de estándares, recomendaciones y orientación y buscarán comprender la relación entre el Código de Prácticas y el material existente de la industria y otras partes interesadas. El mapeo hace que ese ejercicio sea más fácil y, por lo tanto, la implementación del Código de Prácticas es más sencilla.
- Presenta un resumen de cantidad de recomendaciones por Organización/Estándar propuesto por ella. Entre las Organizaciones, se encuentran
    - *IoT Security Foundation*
    - *European Union Agency for Network and Information Security (ENISA)*
    - *Industrial Internet Consortium (IIC)*
    - *GSMA*
    - *Open Web Application Security Project (OWASP)*
    - *IoT Security Initiative*
    - *Online Trust Alliance (OTA)*
    - *Broadband Internet Technical Advisory Group (BITAG)*
    - *Cloud Security Alliance (CSA)*
    - *Internet Engineering Task Force (IETF)*
- Para cada uno de los 13 puntos propuestos por el Código, presenta la siguiente información:
    - Organización
    - Estándar / Nombre de la Recomendación
    - Número de la Recomendación / Sección
    - Recomendaciones extraídas de una fuente asegurada
    - Link al sitio Web

Ambos sucesos descriptos tienen una importancia vital en lo que respecta al aseguramiento de los dispositivos de *IoT*.

Permitirá a los usuarios finales contar con:

- Parámetros de seguridad garantizados por defecto

- El conocimiento el ciclo de vida de sus instalaciones (dispositivos, actualizaciones, etc.)
- Procedimientos o metodologías para la corrección de errores y/o vulnerabilidades.
- Protección de sus datos.

Así mismo, tendrán el aval de organismos gubernamentales que les permitirá cuidar sus derechos.

(Página en Blanco)

CAPITULO VI - Conclusiones y Futuros trabajos

(Página en blanco)

Conclusiones

La *IoT* puede ser un salto cualitativo en el nivel de vida de las personas, generando una oportunidad muy interesante en nuevos negocios que permitirán la optimización de procesos, la toma de decisiones más rápidas y, por qué no, automatizadas en diferentes ámbitos de la vida cotidiana, y traerá nuevos servicios para ofrecer.

Cabe destacar que el volumen de datos y objetos participantes ("cosas") van a generar un gran problema a administrar en lo que respecta a la seguridad de la información vista como conjunto, y que en el presente trabajo se vio acotado sólo a una parte, la autenticación.

También queda evidenciada la vulnerabilidad generalizada en esta tecnología, tanto en dispositivos, como la interconexión o el software que lo administra u opera, aunque por la cantidad y variedad de equipos y "soluciones" que se ofrecen muchas veces hace que dicha vulnerabilidad se vaya incrementando cada día.

La multiplicidad de estándares existentes y la necesidad de ser los "primeros" en implementar soluciones orientadas a la *IoT* también minarán el camino que, tal vez más tarde que temprano, realmente permitan mejorar la calidad de vida mundial.

Los trabajos para que ese tiempo mencionado se vea reducido, deberían estar orientados a la estandarización de los distintos protocolos, servicios y elementos participantes, forzando la implementación de conceptos como "Seguro desde el diseño" y el respeto a la privacidad de los usuarios humanos que, por medio de los objetos que lo rodean o es dueño, participan de este entorno.

Cabe destacar que esa privacidad no está sólo en el momento de la recolección de la información por parte de las "cosas" sino que, también en el uso posterior de los datos recolectados.

Comienzan a aparecer los primeros acercamientos gubernamentales sobre el tema, por lo pronto en Reino Unido – siempre pionera en temas de seguridad, como lo hiciera con la norma *BS7799*[87] – anunciando planes para nuevas leyes que tienen como objetivo proteger los dispositivos de *IoT* de los ataques cibernéticos y el establecimiento de nuevos estándares de industria en ese sentido.

[87] **BS 7799**: Norma británica de seguridad de la información, publicada por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera era un conjunto de buenas prácticas para la gestión de la seguridad de la información -no certificable- y la parte segunda especificaba el sistema de gestión de seguridad de la información -certificable-. La parte primera es el origen de ISO 17799 e ISO 27002 y la parte segunda de ISO 27001.

Si bien, por ahora, se tratan de mesas de trabajo o consulta, pronto serán leyes que permitan asegurar la seguridad desde el diseño, incluyendo características mínimas exigibles para asegurar a todos los usuarios. Es promisorio que los mayores fabricantes del mundo estén participando de estas mesas.

El camino a seguir sería:

- generar un estándar sobre este tema,
- Que los distintos estados y/o mercados comunes se "acoplen" a dicho estándar, de manera de aceptar dispositivos y tecnología asociada que los respete, de manera de garantizar la seguridad.

Podría asimilarse al proceso en el cual surgió la normativa de seguridad de la información generada los ingleses (como hiciera la ISO, convirtiendo una norma inglesa en una con alcance a nivel mundial denominada Norma ISO 17799 – que provenía de la BS7799 y luego 27002) o en paralelo creando uno.

- Divulgar estas normativas hacia los usuarios finales para que éstos las exijan y conozcan los riesgos, cuidados y recomendaciones asociadas.

Futuros trabajos y/o pasos a seguir

Respecto a los futuros trabajos, podrían ser nombrados dos grandes "caminos" a seguir, uno más "cercano", pero no por eso más fácil, asociado a la puesta en práctica o "implementación" del presente trabajo. El otro estaría encaminado en profundizar la investigación que permita conocer las posibilidades que tiene utilizar la tecnología de *Blockchain*[88] y los "Contratos Inteligentes"[89] para ayudar a mejorar la seguridad en la *IoT*.

[88] ***BlockChain***: (En español "cadena de bloques" o bloques encadenados") es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se le añade metainformaciones relativas a otro bloque de la cadena anterior en una línea temporal, de manera que, gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores. Esta propiedad permite su aplicación en un entorno distribuido de manera que la estructura de datos *blockchain* puede ejercer de base de datos pública no relacional que contenga un histórico irrefutable de información. En la práctica ha permitido, gracias a la criptografía asimétrica y las funciones de resumen o hash, la implementación de un registro contable (*ledger*) distribuido que permite soportar y garantizar la seguridad de dinero digital. Siguiendo un protocolo apropiado para todas las operaciones efectuadas sobre la *blockchain*, es posible alcanzar un consenso sobre la integridad de sus datos por parte de todos los participantes de la red sin necesidad de recurrir a una entidad de confianza que centralice la información. Por ello se considera una tecnología en la que la "verdad" (estado confiable del sistema) es construida, alcanzada y fortalecida por los propios miembros; incluso en un entorno en el que exista una minoría de nodos en la red con comportamiento malicioso (nodos *sybil*) dado que, en teoría, para comprometer los datos, un atacante requeriría de una mayor potencia de cómputo y presencia en la red que el resultante de la suma de todos los restantes nodos combinados. Por las razones anteriores, la tecnología *blockchain* es especialmente adecuada para escenarios en los que se requiera almacenar de forma creciente datos ordenados en el tiempo, sin posibilidad de modificación ni revisión y cuya confianza pretenda ser distribuida en lugar de residir en una entidad certificadora.

Implementación del actual trabajo

Las acciones a llevar a cabo serían el asesoramiento y capacitación en los distintos ámbitos de aplicación, de modo que cada uno tenga en cuenta las acciones que tiene que llevar a cabo o solicitar que sean cumplidas.

Puede detallarse las responsabilidades que tendrían que asumir los distintos actores, separándolos por ámbito de aplicación:

Instituciones gubernamentales

Encargadas de fomentar y/o apoyar los procesos de estandarización y crear todo el marco normativo necesario (leyes, disposiciones, etc.) para reforzar la seguridad en el ambiente IoT.

Fabricantes

Los fabricantes deberían, con la mayor celeridad posible, realizar las siguientes acciones:

- Adherir, fomentar e implementar estándares en la tecnología.
- Alertar ante fallas de los productos.
- Establecer reglas claras con la vida útil de los productos.

Instituciones educativas

Realizar las modificaciones necesarias para asegurar que, desde etapas tempranas, y con actualizaciones relacionadas/vinculadas, en los ciclos de enseñanza se puedan estudiar

- principios de la seguridad de la información,
- fomentar el diseño seguro desde la creación del producto o servicio
- fomentar el uso responsable de la tecnología

permitiendo que se puedan generar la dudas e intereses para futuras investigaciones al respecto.

Deberían facilitar, también, la actualización contenidos y/o creación de laboratorios y/o líneas investigativas relacionadas a estos temas.

[89] **"Contratos Inteligentes"**: Es un acuerdo que se ejecuta de manera autónoma y automática entre dos o más agentes en donde una vez definidas las condiciones, las consecuencias se ejecutan de manera automática sin la necesidad de intermediarios. Los contratos inteligentes son programas informáticos, se trata de un fragmento de código virtual que se almacena en una *blockchain*. en donde se define una serie de condiciones (pactadas por las partes) y consecuencias. De esta forma, si se cumple A, entonces automáticamente el contrato ejecutará B. No se requiere de la interpretación ni de la actuación de ningún intermediario. Es capaz de ejecutarse y hacerse cumplir por sí mismo, de manera autónoma y automática, sin intermediarios ni mediadores. Evitan problemas de interpretación al no ser verbal o escrito. Puede ser creado y llamado por personas físicas y/o jurídicas, pero también por máquinas u otros programas que funcionan de manera autónoma.

Usuarios finales

Tomar conciencia de los riesgos asociados a *IoT* conociendo un poco más en profundidad que tecnología es puesta a disposición y cómo es utilizada.

Valorar más la seguridad y la calidad de los productos participantes que el costo, ahorro y/o novedad de los dispositivos a utilizar.

En lo personal

Tendría varios temas a realizar en esta "rama"

- Analizar los estándares y leyes propuestas para conocer la posibilidad de comenzar a cumplir las recomendaciones realizadas y, así, incorporarlas en la vida cotidiana.
- Seguir profundizando con el tema en general e ir incorporando material de clase para ayudar a tomar conciencia sobre el uso de la tecnología y los riesgos que conllevan cuando ésta es mal utilizada.
- Comenzar trabajos con una mayor profundidad con una red de dispositivos para avanzar en otras investigaciones.

Estudio de la Blockchain y los Contratos Inteligentes para mejorar la seguridad de Internet de las Cosas

Analizar si la tecnología de *Blockchain* podría mejorar y/o reemplazar la autenticación conocida, usuario y contraseña, tratando de evitar que los distintos nodos "proveedores de servicios" almacenen las credenciales de cada "cliente".

Para ello podría ser necesario analizar algunos conceptos relacionados a la *Blockchain* son aplicables: Consenso, Distribución y Sin confianza.

Del mismo modo, cabría un estudio particular sobre la aplicabilidad de la descentralización propuesta por esta tecnología aplicada en *IoT*.

CAPITULO VII – Bibliografía

(Página en blanco)

Ashton, K. (Junio de 2009). *That 'Internet of Things' Thing.* Obtenido de RFID Journal: https://www.rfidjournal.com/articles/pdf?4986

Barnes, M. (Agosto de 2017). *Alexa, are you listening?* Obtenido de MWR Labs: https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening/

Brian Rusell, D. V. (2016). *Practical of Internet of Things.* Birmingham,: Pack Publisihng. Obtenido de http://www.allitebooks.org/practical-internet-of-things-security/

Chan, C. (Mayo de 2011). *A Woman Stole A SIM Card And Racked Up $193,187 Worth Of Data Fees.* Obtenido de Gizmodo: https://www.gizmodo.com.au/2011/05/a-woman-stole-a-sim-card-and-racked-up-193187-worth-of-data-fees/

Chris Valasek, C. M. (Julio de 2015). *Remote Exploitation of an Unaltered Passenger Vehicle.* Obtenido de https://ioactive.com: https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf

ComputerWorld. (Julio de 2014). *El 70% de los dispositivos usados en la Internet de las Cosas son vulnerables.* Obtenido de https://cso.computerworld.es: https://cso.computerworld.es/tendencias/el-70-de-los-dispositivos-usados-en-la-internet-de-las-cosas-son-vulnerables

Diario Clarin. (Junio de 2014). *Dispositivos inseguros en las ciudades más grandes del mundo.* Obtenido de www.clarin.com: https://www.clarin.com/sociedad/argentino-demostro-pueden-hackear-semaforos_0_r1UM092qDXx.html

Diaro El Mundo. (Abril de 2018). *Un hacker roba en un casino colándose a través de una pecera.* Obtenido de https://www.elmundo.es/: https://www.elmundo.es/tecnologia/2018/04/17/5ad4a14c46163f1f658b4630.html

ESET. (Enero de 2016). *El troyano BlackEnergy ataca a una planta de energía eléctrica en Ucrania.* Obtenido de https://www.welivesecurity.com: https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/

F-Secure. (Marzo de 2019). *IoT Threat Landscape. Old Hacks, new devices.* Obtenido de F-Secure.com: https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/04/01094545/IoT-Threat-Landscape.pdf

Fundación Telefónica. (Noviembre de 2011). *Smart Cities: un primer paso hacia la internet de las cosas.* Obtenido de https://www.fundaciontelefonica.com/: https://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/101/

Government of UK, Department for Digital, Culture, Media & Sport. (Mayo de 2019). *Plans announced to introduce new laws for internet connected devices.* Obtenido de https://www.gov.uk/: https://www.gov.uk/government/news/plans-announced-to-introduce-new-laws-for-internet-connected-devices

Hillman, M. (2016). *An Overview of ZigBee Networks.* Obtenido de MWR Inforsecurity: https://www.mwrinfosecurity.com/assets/Whitepapers/mwri-zigbee-overview-finalv2.pdf

Hu, F. (2016). *Security and Privacy in Internet of Things (IoTs) Models, Algorithms, and Implementations.* Boca Raton: CRC Press Taylor & Francis Group. Obtenido de http://www.allitebooks.org/security-and-privacy-in-internet-of-things-iots/

INCIBE. (Febrero de 2019). *IoT: protocolos de comunicación, ataques y recomendaciones.* Obtenido de INCIBE - CERT: https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones

Infobae. (Julio de 2015). *La visión del mundo conectado de uno de los 'padres de internet'.* Obtenido de https://www.infobae.com/: https://www.infobae.com/2015/07/14/1741635-la-vision-del-mundo-conectado-uno-los-padres-internet/

Infobae.com. (Enero de 2014). *Heladeras y televisores, origen de un ciberataque.* Obtenido de www.infoabe.com: https://www.infobae.com/2014/01/20/1538288-heladeras-y-televisores-origen-un-ciberataque/

Ingrande, T. (Mayo de 2018). *William Edwards Deming, el propulsor de la Calidad Total.* Obtenido de http://kailean.es: http://kailean.es/william-edwards-deming-el-propulsor-de-la-calidad-total/

IoT News. (Abril de 2019). *F-Secure: IoT attacks doubled in 2018, devices are 'easy prey'.* Obtenido de www.iottechnews.com: https://www.iottechnews.com/news/2019/apr/02/fsecure-iot-attacks-2018-devices-easy/

IOT Analytics. (Enero de 2018). *New Research on 1,600 Enterprise IoT Projects: Upsurge in Smart City and Connected Building Related IoT Projects.* Obtenido de https://iot-analytics.com/global-overview-1600-enterprise-iot-projects/.

IoT News. (Mayo de 2019). *IoT attacks could put a £1bn hole in the UK economy.* Obtenido de https://www.iottechnews.com: https://www.iottechnews.com/news/2019/may/24/iot-attacks-cost-uk-economy-year/

IoT News. (Mayo de 2019). *UK gov announce laws to protect IoT devices from cyberattacks.* Obtenido de https://www.iottechnews.com: https://www.iottechnews.com/news/2019/may/01/uk-gov-laws-protect-iot-devices-cyberattacks/

IoT News. (Abril de 2019). *UK launches 'centre of excellence' for IoT cybersecurity.* Obtenido de https://www.iottechnews.com: https://www.iottechnews.com/news/2019/apr/04/uk-centre-excellence-iot-cybersecurity/

IoT Word on Line. (Julio de 2019). *Las grandes estadísticas del Internet de las Cosas (IoT).* Obtenido de https://www.iotworldonline.es: https://www.iotworldonline.es/las-grandes-estadisticas-del-internet-de-las-cosas-iot/

Islam, S. R. (Junio de 2015). *The Internet of Things for Health Care: A Comprehensive Survey.* Obtenido de IEEE Access: https://www.researchgate.net/publication/280696619_The_Internet_of_Things_for_Health_Care_A_Comprehensive_Survey/citation/download

M. Nabeel, J. Z. (Febrero de 2012). *Cryptographic Key Management for Smart Power Grids - Approaches and Issues.* Obtenido de White Paper: https://arxiv.org/ftp/arxiv/papers/1206/1206.3880.pdf

Mitre. (Julio de 2019). *CVR - Mitre.* Obtenido de https://cve.mitre.org: https://cve.mitre.org/index.htm

OASIS. (Octubre de 2014). *MQTT Specificaction.* Obtenido de http://docs.oasis-open.org/: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html

OWASP. (Mayo de 2019). *IoT Top Ten.* Obtenido de https://www.owasp.org/: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

OWASP. (Mayo de 2019). *IoT Vulnerabilities Project.* Obtenido de https://www.owasp.org: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities

OWASP. (Mayo de 2019). *Proyecto de Áreas de Superficie de Ataque IoT.* Obtenido de https://www.owasp.org/: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Attack_Surface_Areas

Pethuru Raj, A. C. (2017). *The Internet of Things. Enabling Technologies, Platforms, and Use Cases.* Boca Raton: CRC Press Taylor & Francis Group. Obtenido de http://www.allitebooks.org/the-internet-of-things/

Statisa. (s.f.). *https://www.statista.com*. Obtenido de https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Wired. (Junio de 2016). *What we know about friday's massive east coast internet outage.* Obtenido de https://www.wired.com: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

Yuan, M. (Diciembre de 2018). *Conociendo MQTT. ¿Por qué MQTT es uno de los mejores protocolos de red para el Internet de las Cosas?* Obtenido de www.ibm.com: https://www.ibm.com/developerworks/ssa/library/iot-mqtt-why-good-for-iot/index.html