UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Análisis de aspectos de seguridad en arquitecturas IoT

Trabajo Fin de Máster

Máster Universitario en Ingeniería Informática

AUTOR/A: Martínez Patiño, Javier

Tutor/a: Fons Cors, Joan Josep

Cotutor/a: Pelechano Ferragud, Vicente

CURSO ACADÉMICO: 2022/2023

Resumen

Los sistemas IoT están implantados en numerosos ámbitos y cada vez es más común encontrarlos en lugares más dispares, manejando datos o actuando en situaciones en las que incluso la vida de las personas puede depender de ellos.

Sin embargo, lo que a priori es una ventaja, puede convertirse de igual forma en un vector de entrada para actores malintencionados, que pueden encontrar en esta interconexión entre sistemas de todo tipo y con multitud de cometidos un acceso potencial a sistemas críticos y de alto impacto con los que lograr sus fines (ya sean económicos, políticos, afán de reconocimiento, etc.).

Este proyecto presenta un estudio sobre las principales amenazas de seguridad a las que deben hacer frente los sistemas IoT, de modo que pueda servir como guía para fijar los criterios que deben cumplir dichos sistemas para minimizar el riesgo de sufrir un problema de seguridad o, en su defecto, las consecuencias del mismo.

Además de esto, se proporcionan ejemplos y casos prácticos en los que se analizarán los requisitos de seguridad de un sistema propuesto y se darán posibles soluciones para los mismos. Una vez finalizado lo anterior, se extraerán unas conclusiones y lecciones aprendidas que ayudarán al lector a detectar las necesidades de otros sistemas IoT y establecer las medidas necesarias para securizarlo.

Palabras clave: IoT, ciberseguridad, infraestructuras.

Resum

Els sistemes IoT estan implantats en nombrosos àmbits y cada vegada és més comú trobar-los en llocs més diversos, manejant dades o actuant en situacions en les que inclús la vida de les persones pot dependre d'ells.

No obstant, allò que a priori pot semblar un avantatge, pot convertir-se d'igual forma en un vector d'entrada per a actors malintencionats, que poden trobar en aquesta interconnexió entre sistemes de tot tipus i amb multitud de comeses un accés potencial a sistemes crítics i d'alt impacte amb els quals aconseguir la seua finalitat (ja siga econòmica, política, desig de reconeixement, etc.).

Aquest projecte presenta un estudi sobre les principals amenaces de seguretat a les quals han de fer front els sistemes IoT, de manera que puga servir com a guia per a fixar els criteris que han de complir aquests sistemes per a minimitzar el risc de patir un problema de seguretat o, en defecte d'això, les conseqüències d'aquest.

A més d'açò, es proporcionen exemples i diversos casos pràctics en els quals s'analitzaran els requisits de seguretat d'un sistema proposat i es donaran possibles solucions per a aquests. Una vegada fet això, s'extrauran conclusions i lliçons apreses que ajudaran al lector a detectar les necessitats d'altres sistemes IoT i establir les mesures necessàries per a securitzar-lo.

Paraules clau: IoT, ciberseguretat, infraestrcutures

Abstract

IoT systems are deployed in many areas and it is increasingly common to find them in more and more disparate places, handling data or acting in situations in which even people's lives may depend on them.

However, what a prior is an advantage, can also become an entry vector for malicious actors, who can find in this interconnection between systems of all kinds and with a multitude of tasks a potential access to critical and high-impact systems with which to achieve their ends (whether economic, political, desire for recognition, etc.).

This project presents a study of the main security threats faced by IoT systems, so that it can serve as a guide to establish the criteria that such systems must meet in order to minimize the risk of a security problem or, failing that, the consequences of such a problem.

In addition to this, examples and a case study are provided in which the security requirements of a proposed system will be analyzed and possible solutions for the proposed system will be given. Once the above is completed, conclusions and lessons learned will be extracted to help the reader identify the needs of other IoT systems and establish the necessary measures to secure them.

Keywords : IoT, Cybersecurity, infrastructures

Tabla de contenidos

1 Introducción

Desde hace ya varios años, con el auge de los sistemas electrónicos de bajo coste y el aumento de la capacidad y eficiencia de las tecnologías de interconexión a redes de datos (especialmente inalámbricas), han surgido múltiples paradigmas tecnológicos que han tratado de exportar el potencial de los sistemas de información tradicionales al mundo físico hasta niveles nunca antes imaginados.

Tanto es así que en la actualidad podemos encontrar que casi cualquier dispositivo es susceptible de estar conectado a Internet para permitir la interacción remota, automática y/o desatendida con el mismo o la recopilación de datos desde fuentes de lo más variopintas. Esta interacción se lleva a cabo de diferentes formas, ya sea con un sistema de interconexión integrado en el propio diseño del mismo como con dispositivos externos que proporcionan las necesidades de conectividad que permiten aportar estas capacidades a dispositivos que no las incluían entre sus características originales.

Adicionalmente, los dispositivos se integran con multitud de elementos, tanto físicos como componentes software (bancos de datos, inteligencia artificial), paneles de control supervisados por humanos y un largo etcétera, todo ello para aportar agilidad sobre la toma de decisiones y la ejecución de las acciones necesarias en cada una de las situaciones que puedan presentarse.

Sin embargo, lo que a priori puede parecer una ventaja (y de hecho lo es), conlleva problemas que hasta ese momento no existían. Esta interconexión de elementos del mundo físico a los sistemas de información tradicionales los hace susceptibles de atacar actores que en otras circunstancias no tendrían por la dificultad del acceso a estos dispositivos. Por tanto, inherentemente al beneficio de dicha interconexión de estos elementos existen riesgos con los que hay que lidiar desde las fases más iniciales del planteamiento de estas soluciones.

1.1 Motivación

El término "Internet de las Cosas" (también conocido como IoT) se refiere a la comunicación entre objetos comunes que pueden ser identificados de manera única, así como a sus representaciones virtuales a través de una estructura de red convencional, independientemente de su alcance (desde redes locales hasta redes amplias o incluso Internet).

Estos objetos tienen la capacidad de intercambiar información entre sí y, en función de esta, pueden operar de forma autónoma, ya sea supervisados por humanos o incluso sin su intervención. En la actualidad, esta tecnología está en constante crecimiento y la cantidad de dispositivos que pueden integrarse en estos sistemas aumenta de manera significativa. Esto se debe a que está diseñada para funcionar en las redes de comunicación actuales y contribuye a una evolución que acompaña el ritmo de avance de Internet. Con la llegada de la tecnología IPv6, destinada a modernizar la actual IPv4, el número de dispositivos que pueden ser direccionados a través de Internet se expande a 2^{128}, consolidando así al IoT como una solución

de futuro. Como se mencionó anteriormente, los ámbitos de aplicación para el Internet de las Cosas son prácticamente ilimitados: desde el análisis meteorológico y ambiental a la gestión de del tráfico en tiempo real hasta la monitorización de pacientes, pasando por la prevención de desastres naturales o incendios, entre otros. Además, abre un sinfín de nuevas posibilidades de aplicación que antes eran impensables. Gracias al IoT, se facilita el acceso a sistemas que anteriormente resultaban costosos y complejos de diseñar y desplegar. La domótica es un ejemplo claro de cómo se han logrado reducir los costos mediante el aprovechamiento del IoT para implementar esta tecnología, generando además sistemas abiertos que se diferencian de las soluciones propietarias que predominaban en el mercado hasta ahora. Otro ejemplo son las aplicaciones en un aspecto tan importante como la salud, con infinidad de elementos de control corporal, prendas de ropa inteligentes, zapatillas con medidor de valores para optimizar el rendimiento deportivo, medidores de glucosa para diabéticos y un largo etcétera.

Todo esto nos lleva a darnos cuenta de que inherentemente a la cantidad de aplicaciones que puede tener esta tecnología y la revolución que supone, existe un riesgo muy alto de que los atacantes quieran lograr acceso a dichos datos por el valor que pueden tener. Los ataques que pueden sufrir este tipo de sistemas son muy similares a los que puede sufrir un sistema de información tradicional, agrupándolos en ataques dirigidos contra las tres dimensiones de seguridad definidas tradicionalmente: integridad, disponibilidad y confidencialidad.

Si a esto le sumamos que no existe una norma o estándar único que nos ayude a clasificar cada tipo de sistema para discernir los riesgos intrínsecos que puede sufrir por la naturaleza de sus datos, finalidad o arquitectura concretos, los usuarios que quieran aventurarse a iniciar un proyecto con este tipo de tecnologías tienen ante ellos un reto que no siempre es asumible para una gran mayoría con unos requisitos mínimos aceptables.

1.2 Objetivo

El objetivo del proyecto es analizar las amenazas más comunes a las que se pueden enfrentar estos sistemas, proponiendo ejemplos de cada uno y definiendo un mecanismo para gestionar el riesgo que cada una de dichas amenazas puede suponer para los sistemas.

Esta gestión del riesgo dependerá en gran medida el tipo de riesgo, la probabilidad para que se materialice en el sistema, el impacto que podría tener en caso de materializarse y la relación coste/beneficio de las posibles medidas que se podrían tomar en cada caso (entre otros aspectos).

Una vez realizado el análisis, se presentarán casos de uso a los cuales se aplicarán las conclusiones alcanzadas, de modo que se podrá comprobar en un escenario realista la viabilidad técnica de cada una de las medidas definidas.

Con todo ello, será posible identificar los aspectos más relevantes a tener en cuenta a la hora de diseñar arquitecturas o sistemas IoT poniendo el foco en la naturaleza del sistema y los datos que se van a manejar en el mismo.

Este trabajo se centra exclusivamente en analizar amenazas y plantear posibles medidas que mantengan un balance entre coste y beneficio, para que puedan ser implantadas por cualquiera que se plantee el diseño o despliegue de un sistema IoT. Las soluciones para casuísticas muy

complejas que tengan requisitos de seguridad de muy alto nivel podrían no verse reflejadas en el contenido del trabajo. Sería en estos casos realizar un análisis de riesgos pormenorizado del sistema en cuestión, un estudio exhaustivo del diseño del mismo y plantear medidas específicas para cada uno de los casos.

2 Estado del arte

En la actualidad, la ciberseguridad es un tema crítico que afecta a individuos, organizaciones y gobiernos en todo el mundo. Con el aumento constante de las amenazas cibernéticas, se ha convertido en una prioridad proteger la información sensible y garantizar la integridad, confidencialidad y disponibilidad de los datos. Para abordar este desafío, se ha desarrollado una serie de frameworks y estándares de seguridad que sirven como guías y hojas de ruta para implementar medidas efectivas de seguridad de la información.

A continuación, se enumeran los más importantes con una breve descripción de los mismos:

1. **ISO/IEC[1] 27001 y 27002**: La norma ISO/IEC 27001 establece los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI). Junto con la norma ISO/IEC 27002, proporciona un marco sólido para la implementación de prácticas de seguridad de la información. Estos estándares se utilizan en todo el mundo como referencia para la gestión de riesgos de seguridad.
2. **NIST[2] Cybersecurity Framework y Special Publication**: El Framework de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) es ampliamente adoptado en los Estados Unidos. Proporciona un conjunto de mejores prácticas para ayudar a las organizaciones a gestionar y reducir el riesgo cibernético.
3. **COBIT[3] (Control Objectives for Information and Related Technologies)**: COBIT es un marco de gobierno y gestión de TI que incluye un enfoque sólido en la seguridad. Se utiliza para alinear los objetivos de TI con los objetivos de negocio y garantizar la calidad y la confiabilidad de los sistemas de información.
4. **CIS Critical Security Controls[4]**: Los 20 Controles Críticos de Seguridad del Centro de Ciberseguridad (CIS) ofrecen una guía detallada para proteger sistemas y datos críticos. Estos controles se utilizan para mitigar las amenazas cibernéticas más comunes.
5. **IoT Security Frameworks**: Con la proliferación de dispositivos de Internet de las cosas (IoT), se han desarrollado frameworks específicos para garantizar la seguridad en este contexto. Algunos ejemplos incluyen el "IoT Security Foundation Framework" y el "Industrial Internet Consortium (IIC) Industrial Internet Security Framework".

A pesar de la disponibilidad de estos frameworks y estándares de seguridad, los usuarios pueden enfrentarse a desafíos significativos al acceder a esta documentación. La complejidad y longitud de muchas de estas normas y frameworks pueden resultar abrumadoras, especialmente para

1 https://www.iso.org/home.html

2 https://www.nist.gov/

3 https://www.isaca.org/resources/cobit

4 https://www.cisecurity.org/controls

aquellos que no están familiarizados con la terminología de seguridad. Además, algunos de estos documentos pueden estar sujetos a tarifas de adquisición, lo que representa un obstáculo financiero para individuos o pequeñas organizaciones. Este trabajo trata de unificar y simplificar parte de la información que aparece en ellos para ofrecer al lector una guía sencilla de comprender y que ofrezca las medidas de seguridad necesaria.

3 Análisis de la seguridad en la IoT

Como punto de partida sobre el que trabajar y, al haberse comentado anteriormente que los riesgos de seguridad a los que se exponen este tipo de sistemas son muy similares a los de los sistemas de información tradicionales, el planteamiento y las definiciones se basarán en una clasificación derivada de dichos sistemas IT adaptada a las particularidades de este tipo de entornos. Por tanto, las definiciones y conceptos utilizados serán familiares para quien tenga conocimientos sobre seguridad en los sistemas de información convencionales dado que se han utilizado guías de referencia y marcos normativos del entorno IT.

Sin embargo, antes de comenzar con el análisis de los sistemas IoT y sus amenazas, es necesario definir los conceptos básicos sobre qué elementos es fundamental mantener protegidos o seguros para poder definir posteriormente qué es un riesgo. Sin saber cuáles son dichos aspectos y porqué son importantes, es imposible diferenciar los eventos que suponen un riesgo de la simple operativa normal de un sistema, ya que cualquier acción dentro de un sistema provoca un cambio de estado en el mismo, lo que provoca que el sistema pueda realizar la función para la que fue diseñado.

Es fácil darse cuenta que el cambio provocado por la normal operativa al leer el valor de un sensor para tomar la decisión de abrir o no una válvula no está al mismo nivel que el hecho de suplantar y emitir un valor falso en ese mismo sensor para provocar una apertura malintencionada de dicha válvula. Este es un ejemplo claro de pérdida de integridad en el sistema, ya que no es posible asegurar que los datos que se operan son emitidos por el propio sistema, lo que evidentemente provoca un fallo de seguridad en el mismo.

Típicamente, los conceptos clave que definen la seguridad de un sistema se identifican con las siglas *CIA* (o CID en castellano) y son los siguientes: confidencialidad, integridad y disponibilidad.

Existen multitud de definiciones para estos conceptos con gran variedad en la profundidad y el enfoque de los mismos, pero a grandes rasgos se podrían definir de la siguiente forma, tal y como se extrae del glosario del CCN-CERT[9]:

- *Confidencialidad*: propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27000:2014]
- *Disponibilidad*: capacidad de ser accesible y estar listo para su uso a demanda de una entidad autorizada. [UNE-ISO/IEC 27000:2014]
- *Integridad*: propiedad de los datos o información de ser completa, consistente y exacta. [UNE-ISO/IEC 27000:2014]

Es necesario explicar también los diferentes conceptos que se relacionan con la seguridad desde el punto de vista de las eventualidades que pueden sufrir los sistemas y la repercusión de las mismas en el nivel de seguridad final.

- Amenaza: causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. [UNE-ISO/IEC 27000:2014]
- Fallo: error o deficiencia que puede hacer que un sistema sea vulnerable a una amenaza.
- Vulnerabilidad: debilidad de un activo o de un control que puede ser explotada por una o más amenazas. [UNE-ISO/IEC 27000:2014]
- Riesgo: probabilidad de que las amenazas exploten vulnerabilidades de un activo o grupo de activos de información y causen daño. [UNE-ISO/IEC 27000:2014]
- Impacto: consecuencia que sobre un activo tiene la materialización de una amenaza. [Magerit:2012]

De este modo, quedan claros los aspectos de un sistema que deben ser preservados y los sucesos que pueden ocurrir y que tendrían afectación en los mismos, lo que podría desembocar en un problema de seguridad. La forma en la que se podrían materializar dichos problemas de seguridad, así como su impacto y posibles formas de evitarlo se verá en apartados posteriores.

3.1 Categorización de las amenazas

Una vez señalados los conceptos globales que se utilizan y las dimensiones sobre las que se aplican, es necesario definir los riesgos específicos de los sistemas sobre los que se enfoca este trabajo.

Además, hay que establecer categorías para agrupen esas amenazas, para que sea más sencillo comprenderlas y establecer relación entre ellas. Existen multitud de métodos para establecer estas categorías, pero en este caso se va a utilizar una categorización propia correspondiente a las capas del diseño de la arquitectura de los sistemas IoT. El diseño de este tipo de sistema suele dividirse en estas capas o niveles, agrupando los elementos que realizan el mismo cometido en cada una de estas capas. De este modo, es más sencillo organizar el diseño, comprender la interconexión entre las diferentes capas y optimizar dicho diseño para que sea más eficiente y funcional. Por ello, existen multitud de organismos y entidades, como el NIST, el IIC[5] que cuentan con documentación específica sobre el diseño por capas. Incluso en la norma ISO/IEC 27001[13] se hace referencia a dicho modelo y una clasificación de las mismas. En todas ellas, se establecen divisiones muy similares, pero con sus particularidades específicas.

Todas ellas coinciden en establecer tres capas específicas, las cuales se enumeran a continuación:

- Capa de percepción o sensorización.
- Capa de red o transporte.
- Capa de aplicación.

5 https://www.iiconsortium.org/

Sin embargo, esta categorización puede provocar que no se preste especial atención a algunos elementos importantes en sistemas de este tipo al poder clasificarlas entre dos o más categorías indicadas en el listado anterior. Esta problemática ha sido abordada en diversos trabajos académicos[29][3][1] y resuelta añadiendo capas adicionales, por lo que en este caso se ha considerado oportuno añadir dos capas más para acotar cada una de ellas y lograr un nivel de profundidad mayor, lo que permitirá un análisis más exhaustivo y coherente de las amenazas.

De este modo, se han añadido dos capas adicionales, que son las que se mencionan a continuación:

- Capa de middleware.
- Capa de gateway o pasarela

Con todo lo mencionado, se obtiene un nivel de granularidad suficiente para poder realizar una agrupación de las amenazas más precisa en cada una de las categorías. Estas categorías, como se ha comentado, corresponden a una parte del sistema IoT que cumple una función específica y tiene una casuística concreta que se debe conocer antes de profundizar en las amenazas asociadas. Así, se ha generado un mapa conceptual con cada categoría y las amenazas que pueden afectar a cada una.

Figura 1: mapa conceptual de categorías con sus amenazas relacionadas

A continuación, se detalla cada uno de estas capas con una breve explicación sobre sus particularidades:

- **Capa de sensorización**: es uno de los componentes fundamentales de un sistema IoT, ya que es responsable de la recopilación de datos, transmisión de los mismos y actuación sobre el entorno físico. En este nivel, los dispositivos a menudo se encuentran en entornos hostiles y están sujetos a ataques físicos y lógicos siendo los primeros los que más impacto pueden causar a los elementos incluidos en esta capa. Además, también incluye el componente de la actuación, lo que significa que un ataque materializado en algún componente incluido en esta capa tendría la capacidad de

modificar y controlar el entorno físico en el que se colocan los dispositivos. Esto aumenta aún más el riesgo y el impacto de los ataques que afectan a esta capa, lo que puede afectar directamente la seguridad, la privacidad y la integridad física de las personas y de los activos del propio entorno IoT.

- **Capa de red**: es responsable de la comunicación entre dispositivos y la transmisión de datos a través de redes inalámbricas, cableadas o híbridas. En esta capa, los dispositivos IoT interactúan entre sí y con la infraestructura de red para enviar y recibir datos, y para coordinar y controlar el entorno en el que se encuentran. Esta capa es un objetivo atractivo para los atacantes, ya que la explotación de vulnerabilidades puede permitir el acceso no autorizado a los datos y servicios, el control remoto de los dispositivos y la interrupción de la comunicación y el funcionamiento de los sistemas IoT sin necesidad de acceso a los mismos.
- **Capa de middleware**: tiene elementos en común con el anterior, si bien esta categoría se centra más en elementos de red del sistema estrechamente relacionados con las arquitecturas IoT, ya que proporciona una interfaz de comunicación y coordinación entre la capa de aplicación y la capa de sensorización. De esta forma, se facilita la interoperabilidad entre dispositivos y servicios heterogéneos, y se permite el intercambio de datos y servicios a través de múltiples plataformas y sistemas. La explotación de vulnerabilidades en esta capa puede permitir el acceso no autorizado a los datos y servicios, el control remoto de los dispositivos y la interrupción de la comunicación y el funcionamiento de los sistemas
- **Capa de pasarela o gateway**: en esta capa, que también tiene relación con las dos anteriores, se engloban las amenazas relacionadas con los elementos que interconectar las diversas partes del sistema, con especial atención a las interacciones entre segmentos de red claramente diferenciados (como una red de sensores y actuadores con su control independiente y la arquitectura centralizada en la nube donde se encuentra la inteligencia del sistema). Su función principal es, por tanto, es permitir la integración de dispositivos y servicios IoT en la infraestructura de la red, así como proporcionar seguridad y control en la comunicación de los dispositivos y servicios IoT con el resto de redes de comunicaciones.
- **Capa de aplicación**: puede proporcionar una amplia variedad de servicios, desde aplicaciones de monitorización y control de dispositivos hasta servicios de análisis de datos y sistemas de gestión de procesos o control automáticos. Esta capa también puede proporcionar interfaces para interactuar con otros sistemas o servicios, como sistemas de automatización de edificios o sistemas de gestión de energía. A medida que los sistemas IoT se vuelven más complejos, la seguridad en la capa de aplicación se vuelve cada vez más crítica. Los sistemas de aplicaciones IoT son vulnerables a una amplia variedad de ataques, desde ataques de denegación de servicio hasta ataques de inyección de código malicioso y ataques de interceptación de datos.

Todo ello nos permite clasificar los riesgos a los que se enfrentan las tecnologías IoT. Sin embargo, para lograr un conocimiento más profundo de este tipo de sistemas, es necesario también clasificar los diferentes elementos que componen este tipo de sistemas, ya que de esta forma quedan más claras sus necesidades y la criticidad que pueden tener cada una de ellas en el estado final de seguridad del sistema.

3.2 Ejemplificación de las categorías

Para cada una de las capas mencionadas anteriormente, se van a enumerar diferentes ejemplos para dar una idea más aproximada del tipo de dispositivos y su función concreta dentro del sistema.

Capa de sensorización

- *Sensores*: son dispositivos que miden magnitudes físicas como la temperatura, la humedad, la presión, la luz, el sonido, entre otras. Ejemplos de sensores utilizados en IoT incluyen el sensor de temperatura DS18B20, el sensor de humedad y temperatura DHT11 y el sensor de luz BH1750, entre muchos otros.
- *Actuadores*: son dispositivos que permiten modificar el entorno físico en el que se encuentran. Ejemplos de actuadores utilizados en IoT incluyen relés, motores, servomotores, electroimanes, bombas, cerrojos y emisores de infrarrojos, entre muchos otros.
- *Microcontroladores*: son componentes electrónicos que integran un procesador, memoria y otros elementos necesarios para controlar los sensores y actuadores. Algunos de los ejemplos de microcontroladores más utilizados en IoT, sobre todo en sistemas con presupuesto ajustado, son Arduino[6], Raspberry Pi[7] y el ESP32.
- *Protocolos de comunicación*: son los medios por los cuales se envía y recibe información entre los sensores, actuadores y microcontroladores. Ejemplos de protocolos utilizados en IoT incluyen MQTT, CoAP, HTTP y Bluetooth.

Imagen 1: Sensores de ultrasonido (izquierda) y movimiento (derecha)

Capa de red

- *Dispositivos de red*: incluyen routers, switches y puntos de acceso inalámbricos, que permiten la interconexión de diferentes dispositivos IoT y su comunicación con otros dispositivos en la red.

6 https://www.arduino.cc/

7 https://www.raspberrypi.com/

- *Protocolos de comunicación*: se refiere a los estándares de comunicación que permiten a los dispositivos IoT enviar y recibir información en la red. Algunos ejemplos incluyen Wi-Fi, Bluetooth, Zigbee[8], LoRaWAN[9] y MQTT[10].
- *Seguridad de red*: se refiere a las medidas de seguridad que se deben implementar para proteger la red IoT de posibles ataques. Esto puede incluir la encriptación de datos, autenticación de dispositivos y control de acceso a la red.
- *Sistemas de gestión de red*: se refiere a los sistemas de software que permiten la monitorización y el control de la red IoT. Algunos ejemplos incluyen soluciones de gestión de redes IoT basadas en la nube y sistemas de gestión de redes de dispositivos móviles.

Capa de middleware

- *Servidores de middleware*: los servidores de middleware actúan como intermediarios entre los dispositivos IoT y la capa de aplicación, facilitando la comunicación entre elementos que utilizan diferentes tecnologías con las aplicaciones y servicios que dotan al sistema de "inteligencia".

- *API*: la interfaz de programación de aplicaciones (API) proporciona un conjunto de funciones y procedimientos que permiten la comunicación entre los dispositivos IoT y la capa de aplicación.
- *Protocolos de comunicación*: los protocolos de comunicación, como MQTT, CoAP[11], AMQP[12], HTTP, entre otros, se utilizan para la comunicación entre los dispositivos IoT y la capa de aplicación a través del middleware.
- *Gestión de dispositivos*: la gestión de dispositivos es un servicio que se utiliza para la gestión de los dispositivos IoT, como la detección de dispositivos, la configuración, la monitorización y ciertas tareas de la actualización de firmware.
- *Servicios de autenticación y seguridad*: la capa de middleware también puede proporcionar servicios de autenticación y seguridad, como la autenticación de dispositivos, la autenticación de usuarios, la autorización y el cifrado de datos.

Capa de pasarela

- *Dispositivos de enrutamiento*: son dispositivos que se encargan de enrutar los datos entre diferentes dispositivos en la red, incluyendo dispositivos de la capa de sensorización y la capa de middleware. Estos dispositivos también pueden proporcionar funciones de filtrado de datos para reducir la cantidad de tráfico en la red y mejorar la eficiencia.

8 https://csa-iot.org/all-solutions/zigbee/

9 https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/

10 https://aws.amazon.com/es/what-is/mqtt/

11 https://www.rfc-editor.org/rfc/rfc8323.html

12 https://www.amqp.org/

- *Adaptadores de protocolos*: son dispositivos que se encargan de convertir los datos de diferentes formatos y protocolos para asegurar la comunicación adecuada entre los dispositivos que operan con protocolos específicos (por ejemplo, sensores y actuadores en la capa de sensorización) y el resto de capas del sistema. Estos dispositivos pueden utilizarse para conectar elementos que utilizan diferentes protocolos de comunicación, o procesar y adaptar los datos para que sean recibidos en el formato esperado por cada uno de los elementos.
- *Dispositivos de seguridad*: son dispositivos que se encargan de proteger los datos y la red contra posibles amenazas de seguridad, incluyendo ataques cibernéticos. Estos dispositivos pueden proporcionar funciones de autenticación, encriptación y control de acceso para asegurar que los datos se transmitan de forma segura y se almacenen de forma segura.

Capa de aplicación

- *Aplicaciones de usuario final*: son las aplicaciones que utilizan directamente los usuarios finales para interactuar con el sistema IoT. Estas aplicaciones pueden ser aplicaciones móviles, aplicaciones web o software de escritorio.
- *Software de análisis de datos*: es el software que se utiliza para analizar los datos recopilados por los dispositivos IoT y convertirlos en información útil. Estos programas utilizan técnicas de análisis de datos para extraer conocimiento de los datos.
- *Software de gestión de dispositivos*: es el software que se utiliza para administrar los dispositivos IoT. Estos programas pueden ser utilizados para configurar los dispositivos, actualizar el firmware y supervisar el estado de los dispositivos.
- *Plataformas de servicios en la nube*: son plataformas que proporcionan servicios en la nube para el sistema IoT, como almacenamiento, procesamiento y análisis de datos.
- *Interfaz de programación de aplicaciones (API)*: es la interfaz que permite que diferentes aplicaciones y dispositivos se comuniquen entre sí y accedan a los datos y servicios del sistema IoT.

Una vez establecidas las categorías sobre las que se va a realizar el estudio, es posible definir cada una de las amenazas principales recogidas en el mapa conceptual. Adicionalmente es posible que se incluya alguna amenaza que, si bien no se ha incluido en la imagen por no sobrecargar el mapa, puede resultar relevante conocer. Para cada una de las amenazas indicadas, se van a exponer ejemplos y posibles mitigaciones que se deben aplicar para minimizar en la medida de lo posible la materialización de dichas amenazas. Las medidas indicadas están ajustadas al beneficio que proporcionan para ser implementables por la mayoría de actores que deseen construir un sistema IoT con unas garantías de seguridad suficientes, siendo posible implantar sistemas mucho más avanzados y complejos (aunque también caros) para maximizar el nivel de seguridad y reducir el riesgo, pero teniendo en cuenta que alcanzar un nivel de riesgo cero no es posible en ningún sistema.

4 Amenazas de seguridad aplicadas a la IoT

Una vez establecidos los conceptos básicos y la terminología más relevantes, la categorización en capas que se va a usar para realizar el análisis de las vulnerabilidades y la descripción y elementos que conforman cada una de estas capas, es hora de continuar con la clasificación de amenazas que pueden afectar a cada una de las capas.

4.1 Capa de sensorización

La primera categoría corresponde a la capa de sensorización. Esta capa se enfrenta a amenazas específicas debido al tipo de dispositivos que la conforman y el entorno en el que se suelen desplegar. Son dispositivos que disponen de pocos recursos, suministro de energía muchas veces limitado y cuya manipulación puede ser sencilla. Los ataques incluidos en esta categoría y que se detallarán a continuación son los siguientes:

- **Ataque de captura de nodo**
- **Ataque de inyección de código**
- **Ataque de inyección de datos falsos**
- **Ataques de canal lateral**
- **Ataques de interceptación e interferencia**
- **Ataque de drenaje de batería**
- **Ataques en el arranque**

Ataque de captura de nodo

El ataque de captura de nodo es un ataque que compromete uno o más dispositivos IoT al obtener acceso físico o remoto a los mismos y modificar su hardware, software o configuración. Por un lado, los dispositivos afectados por este tipo de ataque son los encargados de recopilar la información para el sistema completo, los efectos para el conjunto pueden ser catastróficos. Un ejemplo claro es la modificación del firmware/software por un atacante para que genere un valor incorrecto que active una alarma, confunda a un operador sobre una situación de peligro simulada o desencadene una rutina de parada de un elemento crítico (como puede ser el cierre de una compuerta física para contener una fuga de un gas peligroso). Por otro lado, en esta capa

también están incluidos los actuadores, lo que implica que un ataque exitoso en esta capa permitiría el control de elementos físicos por parte del atacante.

Dicho ataque está relacionado con los frameworks de referencia mencionados a través de las vulnerabilidades específicas que agrupa de la siguiente forma:

1. **Vulnerabilidad de Firmware No Seguro:**
    - *Relación*: el ataque de captura de nodo puede implicar la modificación del firmware de un dispositivo IoT. Esto se relaciona con la necesidad de asegurar que el firmware de los dispositivos sea seguro y no pueda ser alterado por actores maliciosos.
    - *Referencia*: ISO 27001[13] - Control A.14.2.5 (Seguridad en el desarrollo y soporte de sistemas y aplicaciones), que trata la seguridad en el ciclo de vida del software y el firmware.
2. **Vulnerabilidades de Acceso No Autorizado:**
    - *Relación*: el acceso físico o remoto a dispositivos IoT es una parte fundamental del ataque de captura de nodo. Las vulnerabilidades de acceso no autorizado pueden facilitar este tipo de ataques.
    - *Referencia*: NIST Cybersecurity Framework[8] - Categoría de "Identify" y "Protect" que abordan la gestión de accesos y control de acceso.
3. **Amenazas de Integridad de Datos:**
    - *Relación*: la modificación de hardware, software o configuración en dispositivos IoT puede comprometer la integridad de los datos generados o procesados por esos dispositivos.
    - *Referencia*: OWASP IoT Top Ten[23] - La amenaza de "Manipulación de Dispositivos" se relaciona con la modificación no autorizada de dispositivos IoT.
4. **Vulnerabilidad de Actualizaciones de Firmware Inseguras:**
    - *Relación*: para llevar a cabo un ataque de captura de nodo, los atacantes pueden aprovechar vulnerabilidades en los procesos de actualización de firmware.
    - *Referencia*: Trabajo académico[15] - Este trabajo académico trata sobre la necesidad de asegurar tanto el firmware como el proceso de actualización del mismo.
5. **Vulnerabilidad de Almacenamiento de Claves:**
    - *Relación*: los dispositivos IoT suelen utilizar claves de autenticación y cifrado. La exposición de claves puede permitir a los atacantes modificar la configuración y el software de un dispositivo IoT.
    - *Referencia*: NIST SP 800-183[31] - Este documento del NIST aborda la gestión de claves en sistemas IoT.

6. **Amenazas a la Disponibilidad:**

    - *Relación*: la modificación de dispositivos IoT puede afectar la disponibilidad de servicios y datos. Este ataque puede relacionarse con la amenaza de denegación de servicio (DoS) en sistemas IoT.
    - *Referencia*: NIST Cybersecurity Framework[8] - Categoría "Protect" que se centra en la disponibilidad y medidas de resistencia.

Ataque de inyección de código

El ataque de inyección de código es un ataque que compromete uno o más dispositivos IoT al insertar código malicioso en su software o firmware. Este tipo de ataque puede permitir al atacante tomar el control del dispositivo y modificar su comportamiento. Los efectos para el entorno físico y el medio ambiente pueden ser catastróficos debido a que los sistemas afectados en esta capa son los encargados tanto de tomar datos como de realizar acciones. Un atacante podría realizar acciones tan graves como falsear la información que el dispositivo aporta al resto del sistema e interferir en la toma de decisiones (en la parte de recolección de datos) como ejecutar acciones sobre el entorno de forma arbitraria y remota (en la parte de actuación y dependiendo del sistema concreto).

Dicho ataque está relacionado con los frameworks de referencia mencionados a través de las vulnerabilidades específicas que agrupa de la siguiente forma:

1. **Vulnerabilidad de Inyección de Código:**

    - *Relación*: el ataque de inyección de código se basa en la explotación de vulnerabilidades en la entrada de datos o en la ejecución de comandos no seguros en aplicaciones web o sistemas. Las vulnerabilidades de inyección de código son el punto de entrada para este tipo de ataque.
    - *Referencia*: OWASP Top Ten[23] - La categoría "Inyección" aborda estas vulnerabilidades y proporciona recomendaciones para mitigarlas.

2. **Amenaza de Ejecución de Comandos Maliciosos:**

    - *Relación*: los ataques de inyección de código a menudo involucran la ejecución de comandos maliciosos en sistemas o aplicaciones. Esta amenaza puede tener un impacto significativo en la seguridad de un sistema.
    - *Referencia*: NIST Cybersecurity Framework[8] - Categoría "Detect" y "Respond" que se centran en la detección y respuesta a amenazas como la ejecución de comandos maliciosos.

3. **Vulnerabilidad de Validación de Datos Insuficiente:**

    - *Relación*: la falta de validación adecuada de datos de entrada es una de las causas principales de las vulnerabilidades de inyección de código. La validación de datos insuficiente permite a los atacantes inyectar código malicioso en las aplicaciones.
    - *Referencia*: CWE - CWE-20[4] y CWE-74[6] se relacionan con vulnerabilidades de inyección de código y ofrecen descripciones detalladas.

4. **Amenaza a la Confidencialidad y la Integridad de Datos:**

    - *Relación*: los ataques de inyección de código pueden comprometer la confidencialidad y la integridad de datos, especialmente cuando se utilizan para acceder o modificar datos sensibles.
    - *Referencia*: ISO 27001[13] - Controles relacionados con la confidencialidad e integridad de datos.

Ataque de inyección de datos falsos

El ataque de inyección de datos falsos (FDIA) es un tipo de ataque en el que los atacantes utilizan un dispositivo conectado a la red para emitir datos falsos al sistema. Estos ataques pueden dar como resultado un mal funcionamiento de la aplicación IoT. Los atacantes pueden aprovechar tanto las vulnerabilidades en la red de comunicación de dispositivos IoT inalámbricos para manipular los datos del sensor como las propias características físicas que se están midiendo para generar lecturas incorrectas (como acercar una fuente de calor a un sensor de temperatura o un papel ardiendo a un sensor de humos). Al manipular los datos del sensor y los cálculos que se realizan con estos, pueden lograr que se desencadenen las acciones planeadas como respuesta a las entradas generadas. Estos ataques pueden tener un impacto significativo y ser capaces de interrumpir las actividades normales entre los dispositivos en cualquier red IoT . Por ejemplo, si se inyectan datos falsos en un sistema que controla la distribución de energía eléctrica, podría causar cortes o sobrecargas en la red eléctrica. También se podrían alterar los datos de forma física para desalojar un recinto concreto accionando un sistema de alarma con sensores de humo, fuego o calidad del aire (entre otros muchos).

Este ataque está relacionado con controles y vulnerabilidades recogidas por la documentación de referencia de la siguiente forma:

1. **Vulnerabilidades de Validación de Datos Insuficiente:**

    - *Relación*: el ataque FDIA a menudo se basa en la falta de validación adecuada de los datos de entrada. Las vulnerabilidades de validación insuficiente permiten la inserción de datos falsos.
    - *Referencia*: CWE - CWE-20[4] y CWE-74[6] se relacionan con vulnerabilidades de validación insuficiente y ofrecen descripciones detalladas.

2. **Amenaza a la Integridad de Datos:**

    - *Relación*: el ataque FDIA puede comprometer la integridad de los datos al insertar información falsa o manipulada en sistemas o aplicaciones. Esto afecta directamente la integridad de los datos.
    - *Referencia*: NIST Cybersecurity Framework[8] - Categoría "Protect" que se centra en garantizar la integridad de los datos.

3. **Vulnerabilidad de Inyección de Datos Falsos:**

    - *Relación*: el ataque FDIA implica la inyección de datos falsos en sistemas. Esta es una vulnerabilidad específica que puede ser explotada.

- *Referencia*: OWASP Top Ten[23] - Aunque FDIA no es una categoría específica, se relaciona con el riesgo de "Manipulación de Datos" y "Inyección de Datos".

Ataques de canal lateral

Los ataques de canal lateral son un tipo de ataques que pueden llevar a la filtración de datos sensibles en entornos IoT. Estos ataques pueden basarse en el consumo de energía, ataques con láser, ataques de tiempo o ataques electromagnéticos. Las microarquitecturas de los procesadores y su consumo de energía pueden revelar información sensible a los adversarios. Los chips modernos implementan varias contramedidas para prevenir estos ataques mientras implementan módulos criptográficos. Un atacante podría utilizar un dispositivo para medir el consumo de energía de un dispositivo IoT mientras este realiza operaciones criptográficas. Al analizar los patrones en el consumo de energía, el atacante podría obtener información sobre la clave criptográfica utilizada. Con dicha información, el atacante podría descifrar los datos transmitidos por el dispositivo y acceder a información sensible. En el caso de sistemas IoT críticos, como sistemas de control industrial o dispositivos médicos, esto podría tener consecuencias aún más graves. Por ejemplo, si un atacante obtiene acceso a un sistema de control industrial a través de un ataque de canal lateral en un dispositivo IoT conectado al sistema, podría manipular el funcionamiento del sistema y causar daños materiales o incluso poner en peligro la integridad física de las personas.

Se relaciona con los frameworks de seguridad utilizados como guía de la siguiente forma:

1. **Amenazas a la Privacidad:**
    - *Relación*: los ataques de canal lateral pueden poner en peligro la privacidad al revelar información confidencial, como claves de cifrado o datos de autenticación, a través de canales no autorizados.
    - *Referencia*: ISO 27001[13] - Norma que aborda la privacidad y la protección de datos.
2. **Amenazas a la Criptografía:**
    - *Relación*: los ataques de canal lateral pueden apuntar a vulnerabilidades en algoritmos de cifrado y protocolos de seguridad al aprovechar la información filtrada durante las operaciones criptográficas.
    - *Referencia*: NIST SP 800-57[28] - Documento que proporciona directrices para la selección y uso de algoritmos criptográficos.
3. **Amenazas a la Seguridad Física:**
    - *Relación*: algunos ataques de canal lateral, como los ataques basados en el consumo de energía de un dispositivo, pueden requerir acceso físico a un sistema o dispositivo.
    - *Referencia*: NIST SP 800-82[12] - Guía para la seguridad de sistemas industriales y de control.

Ataques de interceptación e interferencia

Los ataques de interceptación e interferencia están dirigidos a las comunicaciones de diversos nodos desplegados en entornos abiertos. Estos nodos pueden comunicarse entre sí o con una nube utilizando, en la mayor parte de los casos, señales inalámbricas. Los atacantes pueden utilizar dispositivos para interceptar estas señales y capturar los datos transmitidos durante diferentes fases, como la transmisión de datos o la autenticación. Durante un ataque de interceptación, el atacante puede capturar información sensible transmitida por los dispositivos IoT. Esto puede incluir contraseñas, datos personales o información sobre el funcionamiento de los dispositivos. En el caso de un ataque de interferencia, el atacante puede interferir en la comunicación entre los dispositivos IoT y alterar o bloquear la transmisión de datos.

Para ello, se podría utilizar un dispositivo para interceptar las señales inalámbricas transmitidas por un dispositivo IoT mientras este envía datos a otro dispositivo o a un servicio de nube. Al capturar estos datos, el atacante podría obtener acceso a información sensible transmitida por el dispositivo.

El impacto de este tipo de ataques puede ser significativo. Si se obtiene acceso a información sensible, como contraseñas o datos personales, esto puede llevar a la pérdida de privacidad y posibles daños financieros para los usuarios afectados. Además, si se obtiene acceso a dispositivos críticos como sistemas de control industrial o dispositivos médicos, esto podría tener consecuencias aún más graves.

Se relaciona con los frameworks, guías y normativas de seguridad de la siguiente forma:

1. **Amenazas a la Confidencialidad de la Comunicación:**
    - *Relación*: los ataques de interceptación buscan obtener acceso no autorizado a la información transmitida, lo que compromete la confidencialidad de los datos.
    - *Referencia*: ISO 27001[13] - Control A.9 (Gestión de accesos y controles en red) que aborda la confidencialidad de la información durante la transmisión.
2. **Amenazas a la Integridad de Datos:**
    - *Relación*: la interferencia puede alterar la integridad de los datos transmitidos para inyectar datos falsos o modificar los datos legítimos en tránsito.
    - *Referencia*: NIST Cybersecurity Framework[8] - Categoría "Protect" que se centra en la integridad de los datos y la prevención de alteraciones no autorizadas.
3. **Ataques de Man-in-the-Middle (MitM):**
    - *Relación*: los ataques MitM son un subconjunto de ataques de interceptación donde un atacante se interpone en la comunicación entre dos partes y puede capturar o modificar los datos en tránsito.
    - *Referencia*: OWASP Top Ten[23] - La categoría "Comunicaciones inseguras" aborda amenazas MitM.

4. **Amenazas a la Seguridad de Redes Inalámbricas:**
    - *Relación*: la interceptación y la interferencia son amenazas comunes en redes inalámbricas, donde las señales pueden ser capturadas o perturbadas por actores maliciosos.
    - *Referencia*: NIST SP 800-153[11] - Guía para la seguridad de redes inalámbricas.
5. **Protección de Comunicaciones Críticas:**
    - *Relación*: en entornos donde la confidencialidad e integridad de las comunicaciones son críticas, como en infraestructuras críticas, se aplican medidas de seguridad especiales para proteger contra la interceptación y la interferencia.
    - *Referencia*: NIST SP 800-82[12] - Guía para la seguridad de sistemas industriales y de control.

Ataque de drenaje de batería

El ataque de drenaje de batería es un tipo de ataque que se dirige específicamente a uno o varios dispositivos IoT con el objetivo de agotar la batería del dispositivo de forma más rápida a la que debería agotarse. Si un ataque de drenaje de batería se materializa con éxito, puede tener varias consecuencias.

Primero, el dispositivo afectado puede dejar de funcionar correctamente debido a la falta de energía. Esto puede afectar la capacidad del usuario para utilizar el dispositivo y puede requerir que se reemplace la batería o incluso el dispositivo en sí.

Además, si el dispositivo afectado es parte de una red más grande de dispositivos IoT, el ataque puede tener un impacto en toda la red. Por ejemplo, si un sensor de temperatura en una red de sensores deja de funcionar debido a un ataque de drenaje de batería, puede afectar la capacidad de la red para monitorizar y controlar la temperatura en un área determinada.

Se relaciona con estándares y marcos de referencia de la siguiente forma:

1. **Amenazas a la Disponibilidad del Dispositivo:**
    - *Relación*: los ataques de drenaje de batería pueden causar la indisponibilidad del dispositivo al agotar su energía, lo que afecta a su capacidad para funcionar correctamente.
    - *Referencia*: NIST Cybersecurity Framework[8] - Categoría "Protect" que se centra en medidas para garantizar la disponibilidad de sistemas y servicios.
2. **Amenazas a la Integridad del Sistema Operativo:**
    - *Relación*: algunos ataques de drenaje de batería pueden explotar vulnerabilidades en el sistema operativo o en aplicaciones, lo que podría comprometer la integridad de esos sistemas.

- *Referencia*: ISO 27001[13] - Controles relacionados con la gestión de vulnerabilidades y parches de seguridad.

Ataques en el arranque

Los ataques en el arranque representan una amenaza significativa para los sistemas IoT, ya que afectan a los dispositivos desatendidos del sistema, que muchas veces se encuentran en ubicaciones remotas, durante el proceso de arranque del firmware/software. Durante este proceso crítico, los mecanismos de seguridad integrados no están operativos todavía, lo que deja a los dispositivos expuestos a posibles ataques durante el tiempo que dura el arranque. Los atacantes pueden aprovechar estas vulnerabilidades para comprometer la seguridad del dispositivo y acceder a información confidencial o controlar el dispositivo.

Dado que este tipo de dispositivos suelen ser de baja potencia y pueden pasar por ciclos de sueño-despertar, es esencial implementar medidas para asegurar el proceso de arranque o cambio de modo de funcionamiento en estos dispositivos.

El ejemplo más claro de explotación para este tipo de vulnerabilidad sería que un atacante obtiene acceso físico a un dispositivo del sistema, detiene la alimentación eléctrica durante el periodo de tiempo mínimo necesario para conectar un elemento externo al dispositivo y lo reconecta para que el dispositivo se inicie, leyendo secciones de la memoria que contienen información sensible sobre elementos clave del sistema (como datos de la infraestructura, credenciales de acceso, etc).

Se relaciona con los frameworks y estándares de seguridad de la siguiente forma:

1. **Ataques de Reemplazo de Firmware:**
    - *Relación*: los atacantes pueden tratar de reemplazar el firmware original de un sensor IoT con firmware malicioso durante el proceso de arranque, lo que les permite tomar el control del dispositivo.
    - *Referencia*: NIST SP 800-183[31] - Este documento del NIST aborda la gestión de firmware seguro en sistemas IoT.
2. **Firmware Firmado y Autenticación de Arranque:**
    - *Relación*: la implementación de firmas digitales en el firmware y la autenticación de arranque ayudan a garantizar que el firmware no haya sido modificado por terceros no autorizados.
    - *Referencia*: Trabajo académico sobre el firmware y su implicación en la seguridad[15]. Se aborda la problemática del firmware verificado por firma en sistemas IoT.
3. **Protección de Claves Criptográficas:**
    - *Relación*: la protección de las claves criptográficas utilizadas en la autenticación de arranque es esencial para evitar que los atacantes comprometan el proceso de inicio.
    - *Referencia*: ISO 27001[13] - Controles relacionados con la gestión de claves criptográficas.

4. **Detección de Ataques en el Arranque:**
    - *Relación*: implementar mecanismos de detección de comportamiento anómalo durante el arranque puede ayudar a identificar y responder a intentos de ataques en el arranque.
    - *Referencia*: NIST SP 800-61[2] - Guía para la detección de incidentes y respuesta a incidentes.

4.2 Capa de red

La segunda categoría corresponde a la capa de red. Los atacantes suelen prestar especial atención a esta capa, dado que por ella circula gran parte de la información de la que depende el sistema, por lo que un ataque a esta capa ofrece una recompensa sustancial en caso de tener éxito. Los ataques incluidos en esta categoría y que se detallarán a continuación son los siguientes:

- **Ataque de suplantación**
- **Ataque de acceso no autorizado**
- **Ataque de Denegación de Servicio (DoS)**
- **Ataques de datos en tránsito**
- **Ataques de enrutamiento**

Ataque de suplantación

El ataque de suplantación hace referencia a la acción de suplantar o impersonar elementos de red dentro de un sistema y redirigir el tráfico hacia dispositivos maliciosos. Esta forma de suplantación implica engañar o manipular los dispositivos legítimos para enviar o recibir información a elementos controlados por un atacante, lo que puede implicar graves en seguridad y privacidad.

Las implicaciones de los ataques de suplantación en entornos IoT son diversas. En primer lugar, los dispositivos comprometidos pueden ser utilizados como puntos de entrada para llevar a cabo ataques más sofisticados en la red, lo que podría conducir a la filtración de datos confidenciales o al robo de información personal. Además, los dispositivos maliciosos pueden generar tráfico no deseado o incluso interrumpir el funcionamiento normal de la red IoT, afectando la disponibilidad y la confidencialidad de los servicios. Por último, un dispositivo de este tipo operando en una red podría llegar a ser capaz de interferir en procesos críticos para los elementos del sistema, como los procesos de actualización del resto de dispositivos, modificando el software/firmware por otro malicioso que aumente las capacidades del atacante dentro del sistema.

Se relaciona con los estándares y frameworks de seguridad de la siguiente forma:

1. **Ataque de Suplantación (Spoofing):**
    - *Relación*: los ataques de suplantación implican la falsificación de la identidad de un dispositivo o usuario para engañar a otros dispositivos o sistemas en la red.
    - *Referencia*: NIST SP 800-183[31] - Este documento del NIST aborda las amenazas de suplantación y la autenticación en sistemas IoT.
2. **Autenticación y Autorización Segura:**
    - *Relación*: la autenticación sólida y la autorización adecuada son esenciales para prevenir los ataques de suplantación en sistemas IoT, ya que aseguran que solo los dispositivos y usuarios legítimos tengan acceso.
    - *Referencia*: OWASP IoT Top Ten[23] - Aborda la autenticación y la autorización como aspectos críticos de la seguridad en IoT.
3. **Protocolos Seguros de Comunicación:**
    - *Relación*: la elección de protocolos de comunicación seguros, como MQTT con TLS/SSL o CoAP con DTLS[13], ayuda a prevenir la suplantación y proteger la integridad de los datos en tránsito.
    - *Referencia*: Trabajo académico sobre el uso de comunicaciones seguras en sistemas IoT[10]. Trata el uso de protocolos seguros en sistemas IoT y su rendimiento.
4. **Seguridad en el Enrutamiento:**
    - *Relación*: implementar medidas de seguridad, como firewalls y reglas de filtrado, puede ayudar a detectar y bloquear intentos de suplantación.
    - *Referencia*: NIST SP 800-183[31] - Guía para la seguridad de sistemas de red en IoT.
5. **Detección de Anomalías:**
    - *Relación*: la detección de anomalías en la red, como patrones inusuales de tráfico o comportamiento, puede ayudar a identificar intentos de suplantación.
    - *Referencia*: NIST SP 800-137[30] - Menciona la necesidad de detección de anomalías para la seguridad.

Ataque de acceso no autorizado

El ataque de acceso no autorizado se refiere a un tipo de ataque en el que un individuo no autorizado o un adversario obtiene acceso a la red mediante la que se interconectan los dispositivos IoT. El atacante puede permanecer en la red sin ser detectado durante un largo periodo de tiempo. El propósito de este tipo de ataque puede ser de diversa índole, desde robar datos o información valiosa a causar un funcionamiento erróneo o daño a la red y los

13 https://datatracker.ietf.org/doc/html/rfc6347

dispositivos. Esto es así debido a que la red es uno de los puntos de estos sistemas donde es más difícil controlar los elementos, ya que se suele usar infraestructura de comunicaciones de terceros, es una de las vías con un acceso más sencillo.

A consecuencia de que este tipo de ataques se enfocan sobre las infraestructuras de comunicación compartidas y pueden llevarse a cabo de forma remota y, aunque es cierto que si el sistema cuenta con la protección adecuada el nivel de dificultad para este tipo de ataques es alto, cualquiera con un equipo doméstico, acceso a internet y un mínimo de conocimientos podría tratar de comprometer el entorno IoT mediante esta vía.

Se relaciona con las principales guías,normativas y marcos de trabajo de la siguiente forma:

1. **Vulnerabilidad: Falta de Autenticación y Autorización:**
    - *Relación*: la falta de autenticación y autorización sólida es una vulnerabilidad que puede ser explotada para realizar un "ataque de acceso no autorizado" en sistemas IoT.
    - *Referencia*: ISO 27001[13] - Control A.9 (Gestión de accesos y controles en red) que aborda la autenticación y autorización en sistemas de información.
2. **Vulnerabilidad: Falta de Detección de Anomalías:**
    - *Relación*: la falta de sistemas de detección de anomalías puede permitir que los atacantes realicen "acceso no autorizado" sin ser detectados.
    - *Referencia*: NIST SP 800-61[2] - Guía para la detección de incidentes y respuesta a incidentes, que incluye la detección de anomalías como una técnica clave.
3. **Vulnerabilidad: Falta de Control de Acceso:**
    - *Relación*: la falta de un control de acceso adecuado a dispositivos y redes IoT es una vulnerabilidad clave que permite el acceso no autorizado.
    - *Referencia*: OWASP IoT Top Ten[23] - Aborda el control de acceso como uno de los principales riesgos de seguridad en IoT.
4. **Vulnerabilidad: Puertos Abiertos y Servicios No Seguros:**
    - *Relación*: la exposición de puertos abiertos y servicios no seguros en dispositivos IoT aumenta la superficie de ataque y puede conducir a un acceso no autorizado.
    - *Referencia*: NIST SP 800-183[31] - Menciona la importancia de cerrar puertos innecesarios y deshabilitar servicios no seguros en IoT.

Ataque de Denegación de Servicio (DoS)

Un ataque de Denegación de Servicio (DoS) o Ataque Distribuido de Denegación de Servicio (DDoS) se produce cuando un sistema o red es inundado con una cantidad ingente de tráfico malicioso, lo que resulta en la interrupción o la degradación significativa de los servicios. Estos ataques tienen implicaciones graves, tanto a nivel de disponibilidad como de rendimiento, y pueden afectar a partes concretas de los sistemas IoT o al sistema completo.

La principal implicación de los ataques DoS/DDoS es la interrupción de los servicios en línea, lo que puede ocasionar pérdidas económicas, daños a la reputación y frustración a los usuarios finales. Estos ataques pueden paralizar una red o un sistema, negando el acceso legítimo a los usuarios y causando una disminución significativa en la calidad del servicio. Además, los ataques DoS distribuidos (DDoS) son especialmente desafiantes, ya que involucran múltiples dispositivos o computadoras comprometidas como origen del ataque, lo que dificulta su detección y mitigación.

Se relaciona con las amenazas de los principales frameworks de seguridad de la siguiente forma:

1. **Vulnerabilidad: Falta de Protección contra Ataques DoS:**
    - *Relación*: la falta de protección contra ataques DoS es una vulnerabilidad que puede llevar a una interrupción de los servicios en sistemas IoT.
    - *Referencia*: NIST SP 800-183[31] - Este documento del NIST aborda la necesidad de proteger contra ataques DoS en IoT.
2. **Vulnerabilidad: Uso de Protocolos No Resilientes:**
    - *Relación*: la elección de protocolos de comunicación no resistentes a ataques DoS puede exponer sistemas IoT a vulnerabilidades.
    - *Referencia*: NIST SP 800-189[21] - Menciona el uso de protocolos resilientes.
3. **Vulnerabilidad: Falta de Detección de Ataques DoS:**
    - *Relación*: la falta de sistemas de detección de ataques DoS puede dificultar la identificación oportuna de estos ataques en sistemas IoT.
    - *Referencia*: NIST SP 800-61[2] - Guía para la detección de incidentes y respuesta a incidentes, que incluye la detección de ataques DoS como un componente importante.

Ataques de datos en tránsito

Los ataques de datos en tránsito en sistemas IoT tratan de obtener o modificar la información que se transmite entre los diferentes elementos del sistema, de forma que un atacante pueda lograr acceso a los mismos para fines malintencionados o corromperlos para provocar un mal funcionamiento o caída del sistema, de forma total o parcial. Estos ataques de datos en tránsito pueden tener implicaciones significativas en términos de seguridad y privacidad. Los datos sensibles transmitidos entre los dispositivos de IoT y la nube pueden ser interceptados y comprometidos por atacantes malintencionados. Esto puede dar lugar a la filtración de información confidencial, como datos personales, contraseñas o datos empresariales confidenciales. Además, los datos manipulados durante el tránsito pueden resultar en la ejecución de acciones no autorizadas o incluso en la violación de la integridad de los datos.

Se relaciona con las amenazas de los principales frameworks de seguridad de la siguiente forma:

1. **Vulnerabilidad: Comunicaciones sin Cifrado:**
    - *Relación*: la falta de cifrado en las comunicaciones expone los datos en tránsito a riesgos de interceptación o manipulación.
    - *Referencia*: ISO 27001[13] - Control A.13 (Comunicaciones de la información) aborda la necesidad de cifrar las comunicaciones.
2. **Vulnerabilidad: Falta de Autenticación y Autorización:**
    - *Relación*: la falta de autenticación y autorización adecuadas en las comunicaciones permite que los atacantes accedan y manipulen datos en tránsito.
    - *Referencia*: NIST SP 800-183[31] - Este documento del NIST aborda la necesidad de autenticación y autorización en IoT.
3. **Vulnerabilidad: Comunicaciones sin Integridad:**
    - *Relación*: la falta de protección de la integridad de los datos en tránsito permite que los atacantes los modifiquen sin ser detectados.
    - *Referencia*: NIST SP 800-183[31] - Menciona la necesidad de garantizar la integridad de los datos en comunicaciones en IoT.

Ataques de enrutamiento

Los ataques de enrutamiento en sistema de IoT se refieren a la manipulación maliciosa de las rutas de tráfico de red que utilizan los dispositivos, con el objetivo de redirigir el tráfico a través de rutas falsas y no deseadas. Debido a que los sistemas IoT integran gran cantidad de protocolos de red (tanto específicos como estándar y las pasarelas que los conectan), pueden no existir mecanismos de protección integrados en el protocolo. Dos tipos comunes de estos ataques son los ataques de sinkhole (agujero negro) y los ataques de worm-hole (agujero de gusano).

Los ataques de sinkhole implican que un adversario anuncie una ruta de enrutamiento artificial más corta y atraiga a los nodos para que enruten el tráfico a través de ella. Esto permite al atacante interceptar, monitorizar o manipular el tráfico de datos, lo que puede tener consecuencias graves en términos de confidencialidad y disponibilidad de la red.

Por otro lado, los ataques de worm-hole se convierten en una amenaza seria cuando se combinan con otros ataques, como los ataques de sinkhole. Un worm-hole es una conexión fuera de banda entre dos nodos que permite la transferencia de paquetes, comúnmente para establecer una comunicación con un sistema externo controlado por el atacante para exfiltrar información. De esta forma, un atacante puede crear un worm-hole entre un nodo comprometido y un dispositivo en Internet para intentar eludir los protocolos de seguridad básicos en un sistema IoT.

Se relaciona con las amenazas de los principales frameworks de seguridad de la siguiente forma:

1. **Vulnerabilidad: Redirección de tráfico:**
    - *Relación*: el resultado de una suplantación de ruta puede incluir la redirección del tráfico a través de un camino no deseado, lo que podría permitir el espionaje o el análisis malicioso del tráfico.
    - *Referencia*: NIST SP 800-189[21] - Menciona la problemática y consecuencias de las redirecciones no autorizadas en los sistemas.

4.3 Capa de middleware

La tercera categoría corresponde a la capa de middleware. Dada la responsabilidad de los elementos de esta capa de interconectar sistemas de diferente tipo y la información que deben transmitir y, en muchos casos transformar entre formatos de comunicación o protocolos, deben estar preparados frente a amenazas específicas. También es responsable de intercambiar la información entre la capa de aplicación y la de sensorización. Muchas de las amenazas que afectan a la capa de red también se extienden a esta capa, sin embargo, no se incluirán aquí debido a que ya se han tratado en la anterior y se produciría una repetición. Los ataques incluidos en esta categoría y que se detallarán a continuación son los siguientes:

- **Ataques de signature wrapping**
- **Ataque de inyección SQL**
- **Ataques Man in the Middle (MitM)**

Ataques de signature wrapping

Los ataques de signature wrapping (envoltura de firmas) se enfocan en los servicios web utilizados en middleware, donde se utilizan firmas XML. En un ataque de signature wrapping, el atacante trata de romper el algoritmo de firma para ejecutar operaciones o modificar mensajes interceptados al aprovechar vulnerabilidades en SOAP (Protocolo Simple de Acceso a Objetos).

Para ello, el atacante manipula los mensajes SOAP al envolver o alterar las firmas XML. Al hacerlo, puede engañar al sistema y obtener acceso no autorizado o realizar acciones malintencionadas. El objetivo principal del ataque de signature wrapping es eludir la verificación de integridad y autenticidad de los mensajes mediante la manipulación de las firmas XML.

Este tipo de ataque tiene consecuencias graves en el sistema, ya que puede permitir al atacante acceder y modificar datos sensibles, realizar acciones no autorizadas en el sistema o incluso obtener control total sobre el middleware. Además, los ataques de signature wrapping también pueden ser utilizados como punto de partida para otros ataques más sofisticados en el entorno de middleware.

Se relaciona con el sistema de clasificación de amenazas CWE de la forma siguiente:

1. **Amenaza: Improper Verification of Cryptographic Signature (CWE-347)**

- *Relación*: el ataque de "signature wrapping" implica una verificación incorrecta de firmas criptográficas y puede comprometer la autenticidad e integridad de las firmas.
- *Referencia*: CWE-347[5] aborda específicamente la verificación incorrecta de firmas criptográficas en aplicaciones y sistemas.

Ataque de inyección SQL

En un ataque de inyección SQL, un atacante aprovecha las vulnerabilidades en la capa de middleware para insertar comandos SQL maliciosos en las consultas o instrucciones que se envían a los sistemas que procesan la información recibida por el mismo.

En el contexto de IoT, el middleware desempeña un papel crucial en la comunicación y el intercambio de datos entre los dispositivos IoT y las aplicaciones. Sin embargo, si el middleware no está adecuadamente protegido contra ataques de inyección SQL, los atacantes pueden aprovechar estas vulnerabilidades para manipular las consultas y realizar acciones maliciosas.

Las implicaciones de un ataque de inyección SQL en el middleware pueden ser críticas. Los atacantes pueden obtener acceso no autorizado a los datos del sistema IoT, modificarlos o incluso borrarlos por completo. Esto puede tener un impacto significativo en la integridad, confidencialidad y disponibilidad de los datos y el funcionamiento general de los sistemas IoT.

Se relaciona con las amenazas de los principales frameworks de seguridad de la siguiente forma:

1. **Vulnerabilidad: Inyección SQL**
   - *Relación*: la falta de medidas de seguridad adecuadas para prevenir la Inyección SQL puede exponer las aplicaciones a riesgos significativos de seguridad.
   - *Referencia*: OWASP Top Ten[23] - La Inyección SQL se identifica como una de las principales amenazas en la lista y se proporcionan pautas detalladas para prevenirla.
2. **Vulnerabilidad: Exposición de Datos Confidenciales**
   - *Relación*: la inyección SQL puede resultar en la exposición no autorizada de datos confidenciales almacenados en bases de datos.
   - *Referencia*: NIST SP 800-53[18] - Integridad de la información y los sistemas.

Ataques Man in the Middle (MitM)

Los ataques Man in the Middle (MitM) pueden tener un impacto muy significativo. Como se ha dicho, el middleware es una pieza clave en la gestión y el enrutamiento de los datos entre los dispositivos IoT y las aplicaciones, por lo que, si un atacante obtiene acceso no autorizado a esta capa, puede llegar a controlar o manipular la comunicación entre los dispositivos y las aplicaciones.

En un ataque MitM, el atacante trata de interceptar las comunicaciones situándose entre los dispositivos que conforman la red, lo que les puede conllevar el acceso a leer, modificar o incluso falsificar los datos transmitidos.

Las implicaciones de un ataque MitM en el middleware de IoT pueden incluir el acceso no autorizado a los datos sensibles, la manipulación de los datos transmitidos y la interrupción de las comunicaciones entre los dispositivos y las aplicaciones.

Se relaciona con las amenazas de los principales frameworks de seguridad de la siguiente forma:

1. **Vulnerabilidad: Comunicaciones sin Cifrado:**
    - *Relación*: la falta de cifrado en las comunicaciones expone los datos en tránsito a riesgos de interceptación o manipulación.
    - *Referencia*: ISO27001[13] - Control A.13 (Comunicaciones de la información) aborda la necesidad de cifrar las comunicaciones.
2. **Vulnerabilidad: Falta de Autenticación y Autorización:**
    - *Relación*: la falta de autenticación y autorización adecuadas en las comunicaciones permite que los atacantes accedan y manipulen datos en tránsito.
    - *Referencia*: NIST SP 800-183[31] - Este documento del NIST aborda la necesidad de autenticación y autorización en IoT.
3. **Vulnerabilidad: Comunicaciones sin Integridad:**
    - *Relación*: la falta de protección de la integridad de los datos en tránsito permite que los atacantes los modifiquen sin ser detectados.
    - *Referencia*: NIST SP 800-183[31] - Menciona la necesidad de garantizar la integridad de los datos en comunicaciones en IoT.

4.4 Capa de gateway

La cuarta categoría corresponde a la capa de pasarela o gateway. En esta capa están los dispositivos que permiten interconectar diferentes elementos o capas con el resto, para que la información pueda llegar a los puntos del sistema donde sea necesaria. Para ello, debe dirigir el tráfico de forma oportuna y en muchos casos es el elemento que permite realizar actuaciones de mantenimiento sobre los componentes del sistema de difícil acceso, como sensores y actuadores. Considerando todo lo anterior, existen amenazas específicas a las que se debe enfrentar dicha capa para que se pueda asegurar su funcionalidad. Para ello, marcos de seguridad, como el NIST CSF, incluyen amenazas y controles específicos para este tipo de dispositivos, las cuales se han extraído y agrupado en este apartado y se detallan a continuación.

Los ataques incluidos en esta categoría y que se detallarán a continuación son los siguientes:

- **Ataques al secure on-boarding**
- **Ataques a interfaces innecesarias**
- **Ataques al cifrado de extremo a extremo**
- **Ataques a las actualizaciones de firmware**

Ataques al secure on-boarding

El "secure on-boarding" o proceso de incorporación segura es de vital importancia en los sistemas de IoT. Cuando se instala un nuevo dispositivo o sensor en un sistema de IoT, resulta imperativo proteger a las diferentes partes del sistema del resto durante todo el proceso, hasta que los mecanismos de comunicación segura están plenamente operativos. Los gateways actúan como intermediarios entre los nuevos dispositivos y los servicios de gestión, y la práctica totalidad de la información pasa a través de estas pasarelas. Sin embargo, estos elementos son susceptibles a ataques de suplantación y escuchas para capturar las claves de encriptación, siendo especialmente críticas durante el proceso de incorporación y/o integración de nuevos elementos dentro del sistema.

Si un atacante logra acceder de manera no autorizada a esta capa, puede ejercer control o manipulación sobre la comunicación entre los dispositivos y las aplicaciones, o suplantar algunos de ellos, entre otros riesgos. Las implicaciones de un ataque de suplantación en las pasarelas de interconexión de IoT pueden incluir el acceso no autorizado por parte de los atacantes a datos sensibles, la manipulación de los datos transmitidos, la interrupción de las comunicaciones entre los dispositivos y las aplicaciones.

1. **Vulnerabilidad: Proceso de Secure On-boarding Insuficiente**
    - *Relación*: un proceso de secure on-boarding insuficiente puede permitir que dispositivos no autorizados se unan a una red IoT, aumentando el riesgo de acceso no autorizado y ataques.
    - *Referencia*: NIST SP 1800-36A[22] - Proporciona directrices para el Secure On-boarding en sistemas IoT, incluyendo la autenticación segura y la autorización de dispositivos.

Ataques a interfaces innecesarias

Los ataques a interfaces innecesarias en la capa de gateway de los sistemas IoT se refieren a la explotación de vías de comunicación que no están siendo utilizadas o son consideradas innecesarias para la funcionalidad del sistema.

Estas interfaces, sean del tipo que sean y que pueden utilizar infinidad de sistemas de comunicación y protocolos diferentes, actúan como un puente entre los dispositivos IoT y la red externa, y su función principal es facilitar la comunicación y el intercambio de datos entre ambos. Sin embargo, si el gateway incluye interfaces o puertos que no están protegidas adecuadamente o que no se necesitan para el funcionamiento del sistema, se convierten en posibles vectores de ataque para los adversarios.

De este modo, los atacantes pueden aprovechar estas interfaces para infiltrarse en la red y acceder a dispositivos IoT o sistemas conectados. Una vez que obtienen acceso no autorizado, pueden llevar a cabo diversas acciones maliciosas, como la manipulación de datos, la interrupción de la comunicación entre los dispositivos o incluso el robo de información confidencial.

Además, las interfaces innecesarias ofecen a los atacantes una superficie de ataque más amplia, por lo que puede ser más sencillo evadir las medidas de seguridad implementadas en otras partes del sistema y tener un mayor control sobre la red y los dispositivos conectados.

Se relaciona con las normativas y guías de seguridad de la siguiente forma:

1. **Vulnerabilidad: Falta de Segmentación de Red**
    - *Relación*: la falta de segmentación de red puede permitir que atacantes se muevan lateralmente una vez que han comprometido un dispositivo IoT.
    - *Referencia*: NIST Cybersecurity Framework[8] - En el área de "Protect" (Proteger), se enfatiza la segmentación de red como una medida de protección crítica.
2. **Vulnerabilidad: Configuración Predeterminada no Cambiada**
    - *Relación*: el no cambiar la configuración predeterminada en dispositivos IoT puede dejar interfaces abiertas para ataques debido a contraseñas y configuraciones débiles.
    - *Referencia*: IoT Security Foundation Best Practices[14] - Incluye recomendaciones para cambiar las contraseñas y configuraciones predeterminadas en dispositivos IoT.
3. **Vulnerabilidad: Falta de Control de Acceso a Interfaces**
    - *Relación*: la falta de control de acceso adecuado a interfaces puede permitir que usuarios no autorizados accedan y controlen dispositivos IoT.
    - *Referencia*: OWASP IoT Project[24] - Proporciona directrices para la autenticación y autorización adecuadas en dispositivos IoT y sus interfaces.

Ataques al cifrado de extremo a extremo

Los ataques al cifrado de extremo a extremo en un sistema IoT son una preocupación importante, más si cabe que en las aplicaciones IT tradicionales, ya que, debido a la naturaleza de estos sistemas, es común que diferentes elementos que conforman el sistema tengan que hacer traducción de unos protocolos y codificaciones de la información a otros, como aquellos que utilizan los protocolos Zigbee o Z-Wave.

En dichos casos, la información se traduce de un protocolo a otro a través de los gateways, lo que implica que los mensajes cifrados deben ser descifrados y vuelven a cifrarse para la traducción. Esta decodificación en el nivel del gateway abre una posible brecha de seguridad, ya que los datos en su estado descifrado son susceptibles a sufrir filtraciones o manipulaciones.

Los ataques a la falta de cifrado extremo a extremo en un sistema IoT pueden tener implicaciones graves. Los atacantes podrían obtener acceso a los datos en texto plano durante el proceso de traducción en el gateway. Esto podría permitirles leer o modificar información

confidencial, comprometiendo así la privacidad y la confidencialidad, alterando los datos para modificar el comportamiento del sistema.

1. **Vulnerabilidad: Comunicaciones sin Cifrado:**
    - *Relación*: la falta de cifrado en las comunicaciones expone los datos en tránsito a riesgos de interceptación o manipulación.
    - *Referencia*: ISO27001[13] - Control A.13 (Seguridad de las comunicaciones) aborda la necesidad de cifrar las comunicaciones.
2. **Vulnerabilidad: Falta de Autenticación y Autorización:**
    - *Relación*: la falta de autenticación y autorización adecuadas en las comunicaciones permite que los atacantes accedan y manipulen datos en tránsito.
    - *Referencia*: NIST SP 800-183[31] - Este documento del NIST aborda la necesidad de autenticación y autorización en IoT.
3. **Vulnerabilidad: Comunicaciones sin Integridad:**
    - *Relación*: la falta de protección de la integridad de los datos en tránsito permite que los atacantes los modifiquen sin ser detectados.
    - *Referencia*: NIST SP 800-183[31] - Menciona la necesidad de garantizar la integridad de los datos en comunicaciones en IoT.

Ataques a las actualizaciones de firmware

Los ataques a las actualizaciones de firmware en los sistemas IoT representan una preocupación importante en cuanto a la seguridad de los dispositivos en los dispositivos IoT , especialmente aquellos con recursos limitados, ya que no cuentan con una interfaz de usuario o la capacidad de descarga e instalar actualizaciones de firmware desde un servidor mediante protocolos seguros, como ocurre en los sistemas IT convencionales. Por lo tanto, se suelen utilizan los gateways como intermediarios para descargar y aplicar estas actualizaciones cuando se realizan mediante despliegues OTA (Over the Air).

Los ataques a las actualizaciones de firmware pueden comprometer la seguridad del sistema IoT si no se implementan medidas adecuadas. Los atacantes pueden aprovechar las vulnerabilidades en el proceso de descarga y aplicación de actualizaciones de firmware para introducir código malicioso en los mismos, interrumpir el proceso de actualización o incluso realizar ataques de suplantación.

Dicho ataque está relacionado con los frameworks de referencia mencionados a través de las vulnerabilidades específicas que agrupa de la siguiente forma:

1. **Vulnerabilidad de Firmware No Seguro:**
    - *Relación*: el ataque de captura de nodo implica modificar el firmware de un dispositivo IoT. Esto se relaciona con la necesidad de asegurar que el firmware de los dispositivos sea seguro y no pueda ser alterado por actores maliciosos.

- *Referencia*: ISO27001[13] - Control A.14.2.5 (Seguridad en el desarrollo y soporte de sistemas y aplicaciones), que trata la seguridad en el ciclo de vida del software y el firmware.

2. **Vulnerabilidad de Actualizaciones de Firmware Inseguras:**
    - *Relación*: para llevar a cabo un ataque de captura de nodo, los atacantes pueden aprovechar vulnerabilidades en los procesos de actualización de firmware.
    - *Referencia*: Trabajo académico sobre actualización segura en IoT[15] - Se aborda la problemática del firmware verificado por firma en sistemas IoT.

4.5 Capa de aplicación

La quinta categoría corresponde a la capa de aplicación. Dado que es la capa más similar a los sistemas IT, ya que es la más abstracta del sistema IoT debido a los elementos que la integran y la funcionalidad de la misma, existen infinidad de marcos de trabajo de organismos y entidades reconocidas que ofrecen metodologías de análisis de amenazas frente a esta capa. Sin embargo, por mantener coherencia con el resto de marcos utilizados, se utilizarán como referencia principal las amenazas incluidas por el NIST y el OWASP, de las cuales se han extraído los ataques que pueden afectar a esta capa, que se detallan a continuación. Los ataques incluidos en esta categoría y que se detallarán a continuación son los siguientes:

- **Ataques de robo de información**
- **Ataques a los sistemas de control de acceso**
- **Ataques de interrupción de servicio**
- **Ataques de inyección de código**
- **Ataques de interceptación de datos**

Ataques de robo de información

Los ataques de robo de información en la capa de aplicación de los sistemas IoT representan una grave amenaza para la confidencialidad y privacidad de los datos críticos y privados manejados por estas aplicaciones. Dichas aplicaciones reciben y transmiten la práctica totalidad de los datos que se utilizan en el sistema, por lo que lograr acceso a las mismas permite al atacante acceder a dicha información desde un punto unificado. Un ataque a cualquier aplicación del sistema puede suponer una fuga de información crítica, sobre todo si este afecta a la base de datos de la misma, que es donde se almacena la información.

El robo de información en las aplicaciones de IoT puede tener consecuencias significativas, ya que los datos sensibles pueden ser interceptados o extraídos de los sistemas y utilizados de manera malintencionada. Esto puede comprometer la privacidad de los usuarios, exponer información confidencial, como datos de identificación personal o datos de salud, y llevar a posibles fraudes o suplantaciones de identidad.

Se relaciona con las normativas y guías de seguridad de la siguiente forma:

1. **Vulnerabilidad: Exposición de Datos Confidenciales**
    - *Relación*: exposición no autorizada de datos confidenciales.
    - *Referencia*: NIST SP 800-53[18] - Integridad de la información y los sistemas**.**
2. **Vulnerabilidad: Falta de Control de Acceso**
    - *Relación*: falta de control de acceso adecuado.
    - *Referencia*: OWASP Top Ten[23] - Proporciona directrices para la autenticación y autorización adecuadas.
3. **Vulnerabilidad: Inyección SQL**
    - *Relación*: falta de medidas de seguridad para prevenir inyecciones SQL.
    - *Referencia*: OWASP Top Ten[23] - La Inyección SQL se identifica como una de las principales amenazas en la lista y se proporcionan pautas detalladas para prevenirla.
4. **Vulnerabilidad: Exposición de Datos Confidenciales**
    - *Relación*: la inyección SQL puede resultar en la exposición no autorizada de datos confidenciales almacenados en bases de datos.
    - *Referencia*: NIST SP 800-53[18] – Integridad de la información y los sistemas.

Ataques a los sistemas de control de acceso

Los ataques a los sistemas de control de acceso en la capa de aplicación representan una amenaza crítica para la seguridad y la integridad de los datos y las cuentas. El control de acceso es un mecanismo de autenticación y autorización que permite que solo los usuarios o procesos legítimos accedan a los datos o cuentas en un sistema, y con qué nivel de permisos realizan dichos accesos. Sin embargo, cuando el control de acceso se ve comprometido, toda la aplicación de IoT se vuelve vulnerable a ataques de todo tipo.

Los ataques al control de acceso pueden tener consecuencias significativas, ya que permiten a los atacantes obtener acceso no autorizado a los datos o cuentas en un sistema IoT. Una vez que los atacantes logran comprometer el control de acceso, pueden llevar a cabo una variedad de acciones maliciosas, como la manipulación de datos, el robo de información confidencial o incluso la interrupción del funcionamiento normal de la aplicación.

Se relaciona con los marcos de seguridad y guías de la siguiente forma:

1. **Vulnerabilidad: Explotación de vulnerabilidades de autenticación débil**
    - *Relación*: autenticación y control de acceso.
    - *Referencia*: OWASP Top Ten[23] - Lista de las 10 Principales Vulnerabilidades de Aplicaciones Web.
2. **Vulnerabilidad: Ataques de fuerza bruta o ataques de diccionario en contraseñas**
    - *Relación*: autenticación segura.

- *Referencia*: NIST SP 800-63B[20] - Directrices de autenticación digital.

3. **Vulnerabilidad: Uso indebido de credenciales robadas**
    - *Relación*: control de acceso y autorización.
    - *Referencia*: ISO27001[13] - Control A.9.2.3 (Control de acceso a sistemas y aplicaciones).
4. **Vulnerabilidad: Bypass de mecanismos de autenticación**
    - *Relación*: autenticación y control de acceso.
    - *Referencia*: OWASP Top Ten[23] - Lista de las 10 Principales Vulnerabilidades de Aplicaciones Web.
5. **Vulnerabilidad: Suplantación de identidad en el nivel de red**
    - *Relación*: seguridad de la red.
    - *Referencia*: NIST SP 800-53[18] - Control AC-3 (Control de autenticación).

Ataques de interrupción de servicio

Los ataques de interrupción de servicio en la capa de aplicación están diseñados para interrumpir o degradar el funcionamiento normal de las aplicaciones, que usualmente son las utilizadas por los usuarios del sistema IoT para visualizar datos, tomar decisiones estratégicas o incluso aplicar cambios y gestionar el propio sistema. Todo ello puede tener consecuencias graves en términos de pérdida de productividad, daños financieros y compromiso de la seguridad y operativa del sistema completo.

Estos ataques pueden llevarse a cabo utilizando diferentes técnicas, como el envío masivo de solicitudes maliciosas para saturar los recursos del sistema, el agotamiento de ancho de banda o la inyección para provocar errores en la aplicación. Los atacantes buscan explotar vulnerabilidades para alterar el funcionamiento normal, impedir el acceso legítimo a los servicios y causar daño.

Se relacionan con las guías y normativas de seguridad de la siguiente forma:

1. **Vulnerabilidad: Ataque de denegación de servicio distribuido (DDoS)**
    - *Relación*: disponibilidad y resistencia ante ataques.
    - *Referencia*: NIST SP 800-53[18] - Control CP-2 (Continuidad de la operación).
2. **Vulnerabilidad: Agotamiento de recursos de red o servidor**
    - *Relación*: gestión de recursos y capacidad.
    - *Referencia*: ISO27001[13] - Control A13.1.2 (Seguridad de los servicios en red).
3. **Vulnerabilidad: Explotación de vulnerabilidades para bloquear el servicio**
    - *Relación*: protección contra vulnerabilidades y amenazas.
    - *Referencia*: OWASP Top Ten[23] - Lista de las 10 Principales Vulnerabilidades de Aplicaciones Web (sección sobre explotación de vulnerabilidades).

Ataques de inyección de código

Los ataques de inyección de código son técnicas maliciosas en las cuales los atacantes aprovechan vulnerabilidades en la capa de aplicación del sistema IoT para insertar y ejecutar scripts o código no autorizado. Estos ataques generalmente se llevan a cabo mediante la explotación de deficiencias en los controles de código, permitiendo la inserción de scripts maliciosos en sitios web o aplicaciones utilizadas por los usuarios del sistema. Un ejemplo común de este tipo de ataque es el XSS (cross-site scripting), donde se inyecta un script malicioso en un sitio web de confianza, lo que puede resultar en la toma de control de una cuenta de IoT y paralizar el sistema.

Este tipo de ataques tienen implicaciones significativas en la seguridad y el funcionamiento del sistema. Algunas de las implicaciones clave son la posibilidad de ejecutar operaciones no autorizadas o maliciosas que comprometen la integridad y confidencialidad de los datos. También existe el riesgo de compromiso de cuentas de IoT, lo que puede llevar a la manipulación de datos, robo de información confidencial o interrupción del sistema. Por último, otra de las implicaciones que más riesgo comportan es el daño a la reputación y confianza de los usuarios en el sistema IoT, lo que puede resultar en pérdida de clientes y oportunidades comerciales.

Se relacionan con las guías y normativas de seguridad de la siguiente forma:

1. **Vulnerabilidad: Inyección de SQL**
    - *Relación*: protección contra vulnerabilidades de inyección.
    - *Referencia*: OWASP Top Ten[23] - Lista de las 10 Principales Vulnerabilidades de Aplicaciones Web (sección sobre inyección de SQL).
2. **Vulnerabilidad: Inyección de comandos**
    - *Relación*: protección contra vulnerabilidades de inyección.
    - *Referencia*: OWASP Top Ten[23] - Lista de las 10 Principales Vulnerabilidades de Aplicaciones Web (sección sobre inyección de comandos).
3. **Vulnerabilidad: Inyección de scripts maliciosos (XSS)**
    - *Relación*: protección contra vulnerabilidades de inyección.
    - *Referencia*: OWASP Top Ten[23] - Lista de las 10 Principales Vulnerabilidades de Aplicaciones Web (sección sobre XSS).
4. **Vulnerabilidad: Inyección de código en aplicaciones móviles**
    - *Relación*: protección contra vulnerabilidades de inyección en aplicaciones móviles.
    - *Referencia*: OWASP Mobile Application Security[25] - Guía de pruebas de seguridad para aplicaciones móviles.
5. **Vulnerabilidad: Inyección de código en servicios web**
    - *Relación*: protección contra vulnerabilidades de inyección en servicios web.
    - *Referencia*: OWASP Web Security Testing Guide[26] - Guía de pruebas de seguridad para servicios y aplicaciones web.

6. **Vulnerabilidad: Inyección de código en aplicaciones de escritorio**
    - *Relación*: protección contra vulnerabilidades de inyección en aplicaciones de escritorio.
    - *Referencia*: CWE-94[7] - Lista de debilidades de seguridad en el código (CWE-94: Code Injection).

Ataques de interceptación de datos

Los ataques de interceptación de datos se refieren a la acción maliciosa de los atacantes que utilizan aplicaciones de análisis de tráfico (sniffers) para monitorizar el tráfico de red en las aplicaciones IoT. Estos ataques tienen como objetivo obtener acceso a datos confidenciales de los usuarios aprovechando la falta de implementación de protocolos de seguridad adecuados para prevenirlos.

Estos ataques pueden tener implicaciones graves en la privacidad de los sistemas IoT, siendo el más destacable el acceso a datos confidenciales transmitidos a través de la red, como información personal, contraseñas u otra información sensible. Si un atacante lograra acceso a estos datos, podría incluso suplantar la identidad de un usuario, o ejecutar acciones malintencionadas impersonando a un usuario con permisos de administrador. Por último, cabe considerar el potencial riesgo para el espionaje industrial, debido a que los datos interceptados pueden contener información valiosa sobre procesos industriales, estrategias comerciales o secretos de propiedad intelectual, lo que puede dar lugar a pérdidas económicas significativas.

Se relaciona con estándares y marcos de referencia de seguridad de la siguiente forma:

1. **Vulnerabilidad: Interceptación de datos mediante Sniffing de red**
    - *Relación*: privacidad y confidencialidad de datos.
    - *Referencia*: NIST SP 800-53[18].
2. **Vulnerabilidad: Sniffing de datos en una red inalámbrica no segura (Wi-Fi)**
    - *Relación*: seguridad de redes inalámbricas.
    - *Referencia*: NIST SP 800-97[19] - Guía de seguridad de redes inalámbricas.
3. **Vulnerabilidad: Interceptación de tráfico en una red corporativa**
    - *Relación*: seguridad de la red.
    - *Referencia*: ISO 27001[13] - Control A13.1.2 (Seguridad de los servicios en red).
4. **Vulnerabilidad: Monitorización de tráfico de red en aplicaciones móviles**
    - *Relación*: seguridad de aplicaciones móviles.
    - *Referencia*: OWASP Mobile Security Testing Guide[25] - Guía de pruebas de seguridad para aplicaciones móviles.

5 Securización de soluciones IoT

Esta sección se enfoca en proporcionar un conjunto completo de medidas de seguridad específicas destinadas a securizar cada una de las amenazas de las capas en las que se han dividido los elementos de los sistemas IoT, de acuerdo a la categorización del apartado 4. Esto garantiza una respuesta estratégica y efectiva a las amenazas, alineada con la estructura del sistema IoT, con el objetivo primordial de salvaguardar la integridad, confidencialidad y disponibilidad de los datos. Cada una de estas medidas ha sido extraída de las fuentes de referencia o diseñada a partir de las mismas.

Las medidas aportadas tienen una doble finalidad. Por un lado, ofrecer una guía para que su implantación mejore la seguridad de los sistemas IoT independientemente de los mismos. Por otro, ofrecer al lector una visión de las necesidades que pueden tener los sistemas a la hora de aplicar medidas de seguridad, de forma que este sea capaz de ampliar también su conocimiento sobre las amenazas que estas minimizan.

5.1 Capa de sensorización

Medidas contra los ataques de captura de nodo

Los ataques de captura de nodo, que tienen como objetivo comprometer dispositivos IoT individuales, representan una amenaza constante para la integridad y la confidencialidad de los datos. Para mitigar el riesgo de un ataque de captura de nodo, es esencial implementar una serie de medidas de seguridad específicas en la capa de dispositivos IoT.

1. **Identificar y Clasificar Dispositivos**: el primer paso crítico es identificar y clasificar los dispositivos de la capa en cuestión. Esto implica un inventario exhaustivo de todos los dispositivos IoT, asignándoles una categoría basada en su función y relevancia para la operación general del sistema. Esta clasificación permite priorizar la seguridad según el valor que cada dispositivo aporta al ecosistema IoT.
2. **Establecer una Línea Base del Tráfico**: para detectar posibles anomalías que podrían indicar un ataque de captura de nodo, es esencial establecer una línea base del tráfico normal generado por los dispositivos. Esto implica monitorizar y registrar el tráfico típico de los dispositivos en condiciones normales de funcionamiento. Cualquier desviación significativa de esta línea base puede activar alertas para una acción inmediata.
3. **Autenticación y Cifrado**: para proteger tanto el acceso con cable como inalámbrico a los dispositivos IoT, se deben implementar medidas de autenticación fuerte entre las partes y cifrado de extremo a extremo en las comunicaciones. Esto asegura que solo los usuarios autorizados puedan acceder a los dispositivos y que los datos transmitidos sean ininteligibles para posibles atacantes que intenten interceptarlos.

4. **Ubicación Segura y Restricción de Acceso**: colocar físicamente los dispositivos en lugares seguros es esencial para evitar la captura de nodos. Esto significa almacenar los dispositivos en áreas de acceso restringido y controlado, donde solo personal autorizado pueda ingresar. Además, se deben implementar medidas físicas de seguridad, como cerraduras, alarmas y cámaras de seguridad, para prevenir robos o sabotajes.
5. **Verificación de Integridad**: utilizar los mecanismos proporcionados por los fabricantes para verificar la integridad del hardware y del software/firmware es crítico. Esto incluye la aplicación de actualizaciones de seguridad y parches recomendados por el fabricante para protegerse contra vulnerabilidades conocidas. La verificación de integridad también implica la detección de cambios no autorizados en el software o el hardware que podrían indicar manipulación maliciosa.

Medidas contra los ataques de inyección de código

Los ataques de inyección de código buscan explotar vulnerabilidades en los dispositivos IoT, permitiendo a los atacantes ejecutar código malicioso y tomar el control. A continuación, se examinará un listado de medidas correctivas cruciales para proteger los dispositivos IoT contra esta peligrosa amenaza.

1. **Utilizar Software y Firmware Actualizados**: mantener el software y firmware de los dispositivos IoT actualizados es fundamental. Esto implica aplicar las últimas actualizaciones y parches proporcionados por el fabricante. Las actualizaciones suelen abordar vulnerabilidades conocidas y mejorar la seguridad del dispositivo, reduciendo la exposición a posibles ataques de inyección de código.
2. **Establecer una Línea Base del Comportamiento Normal**: para detectar posibles anomalías que indiquen un ataque de inyección de código, es esencial establecer una línea base del comportamiento normal del dispositivo. Esto implica monitorizar y registrar el funcionamiento típico del dispositivo en condiciones normales de operación. Cualquier desviación significativa de esta línea base puede ser un indicio de un ataque.
3. **Proteger el Acceso con Autenticación y Cifrado**: la autenticación sólida y el cifrado de las comunicaciones son fundamentales para proteger el acceso al dispositivo contra la inyección de código malicioso. Esto asegura que solo usuarios autorizados puedan interactuar con el dispositivo y que las comunicaciones estén protegidas contra posibles ataques de interceptación y manipulación.
4. **Restringir el Acceso a la Interfaz de Programación**: limitar el acceso a la interfaz de programación del dispositivo a usuarios autorizados y de confianza es esencial para prevenir inyecciones de código malicioso. Esto se logra mediante la implementación de controles de acceso y políticas de seguridad que restringen el acceso a la interfaz solo a aquellos que tienen una necesidad legítima.
5. **Verificar la Integridad del Software/Firmware**: utilizar los mecanismos proporcionados por el fabricante para verificar la integridad del software y firmware es una práctica esencial. Estos mecanismos pueden incluir firmas digitales o hash de archivos para detectar cualquier modificación no autorizada. La verificación constante garantiza que el software y el firmware no hayan sido comprometidos.

Medidas contra los ataques de inyección de datos falsos

El ataque de inyección de datos falsos, como se ha comentado, tiene como objetivo corromper la integridad de los datos recopilados por dispositivos IoT, lo que puede tener consecuencias graves. A continuación, se detalla un listado de medidas diseñadas para proteger nuestros dispositivos IoT contra la inyección de datos falsos y garantizar la fiabilidad de la información que generan y procesan.

1. **Asegurar la Integridad y Privacidad de los Datos Transmitidos**: garantizar la integridad y privacidad de los datos es esencial para prevenir la inyección de datos falsos. Esto se logra mediante el uso de cifrado robusto y autenticación fuerte en las comunicaciones entre dispositivos IoT y las fuentes generadoras de datos. El cifrado protege los datos en tránsito, mientras que la autenticación asegura que solo las partes autorizadas puedan acceder y modificar los datos.
2. **Mantener el Firmware y Software Actualizado**: mantener actualizado el firmware y el software de los dispositivos IoT es crucial para protegerlos contra vulnerabilidades conocidas que podrían ser explotadas para inyectar datos falsos. Las actualizaciones regulares proporcionadas por el fabricante suelen incluir correcciones de seguridad y mejoras que fortalecen la resistencia del dispositivo contra ataques.
3. **Proteger contra Manipulaciones Físicas**: la protección física de los dispositivos IoT es esencial para prevenir la manipulación de datos. Esto implica el uso de carcasas resistentes a manipulaciones y la instalación de dispositivos en lugares seguros y de difícil acceso. Estas medidas ayudan a prevenir la manipulación física de los dispositivos y garantizan la integridad de los datos que generan.
4. **Generar una Línea Base para los Datos Recopilados**: establecer una línea base para los datos recopilados por los sensores IoT es una estrategia importante para detectar la inyección de datos falsos. Al monitorizar constantemente las lecturas de los sensores y compararlas con esta línea base, es posible identificar picos o lecturas anómalas que puedan indicar un ataque en curso.
5. **Utilizar Redundancia en la Medición**: para tener una mayor confiabilidad en la precisión de los datos recopilados, se puede implementar la redundancia en la medición. Esto se logra utilizando múltiples sensores en ubicaciones cercanas y con diferentes principios físicos para realizar una doble comprobación de los datos. Si los datos de diferentes sensores no coinciden, puede indicar una posible inyección de datos falsos que requiere una revisión y verificación adicionales.

Medidas contra los ataques de canal lateral

Los ataques de canal lateral, como se ha definido en el apartado 4, aprovechan información indirecta, como consumo de energía o radiación electromagnética, para comprometer la privacidad y la seguridad de los datos, representan una seria vulnerabilidad. A continuación, se enumeran algunas medidas que pueden minimizar o eliminar dicha amenaza.

1. **Reducción de Señales Emitidas con Apantallamiento y Enmascaramiento**: para reducir la exposición a ataques de análisis lateral, es importante aplicar técnicas de apantallamiento que disminuyan las señales electromagnéticas y acústicas emitidas por los dispositivos IoT. Esto puede lograrse mediante la adopción de materiales y técnicas

de diseño que minimicen la radiación electromagnética. Además, el enmascaramiento de señales, como la inserción de señales de ruido o la modificación de las características de las señales, puede dificultar la interpretación de los datos capturados por los atacantes.

2. **Instalación de Sistemas de Detección de Ataques de Canal Lateral**: para detectar posibles ataques de canal lateral, es fundamental implementar sistemas de seguridad adicionales y procesos de monitorización especializados. Estos sistemas pueden incluir sensores de detección de emisiones electromagnéticas, análisis de tiempo y potencia, y técnicas de detección de patrones anómalos. La detección temprana de actividad sospechosa permite tomar medidas preventivas antes de que se produzca una fuga de datos.
3. **Utilización de Técnicas de Autenticación Multifactor, Cifrado PKI y Ofuscación de Datos**: para mitigar el riesgo de una fuga de datos causada por ataques de análisis lateral, es crucial implementar medidas sólidas de seguridad. La autenticación multifactor agrega una capa adicional de protección al requerir múltiples métodos de autenticación para acceder a los dispositivos. El cifrado PKI (Infraestructura de Clave Pública) asegura la confidencialidad de las comunicaciones, mientras que la ofuscación de datos dificulta la comprensión de la información interceptada. Estas técnicas combinadas ayudan a proteger tanto la autenticidad como la confidencialidad de los datos en dispositivos IoT.

Medidas contra los ataques de interceptación e interferencia

Los ataques de interceptación e interferencia buscan comprometer la integridad y la confidencialidad de las comunicaciones en los dispositivos IoT, socavando así su funcionalidad y su seguridad. A continuación, se muestra una serie de medidas que tienen el objetivo de proteger los sistemas IoT contra este tipo de ataques.

1. **Proteger la Privacidad y la Integridad de los Datos**: la protección de la privacidad de los clientes, la integridad y confidencialidad de los datos, y la seguridad de la infraestructura y los dispositivos IoT son esenciales. Esto se logra mediante la implementación de prácticas de seguridad sólidas, como el cifrado de datos en reposo y en tránsito, el control de acceso basado en roles y la autenticación multifactor. Garantizar la disponibilidad de los servicios proporcionados por el ecosistema IoT también implica contar con planes de recuperación ante desastres y redundancia en la conectividad.
2. **Evaluación de Vulnerabilidades en Módulos y Protocolos de Comunicación**: es fundamental realizar evaluaciones exhaustivas de seguridad en los módulos y protocolos de comunicación utilizados en el entorno IoT. Esto ayuda a identificar y remediar posibles vulnerabilidades que podrían ser explotadas por atacantes para recuperar información sensible, como contraseñas, claves de cifrado y certificados. La evaluación de vulnerabilidades debe ser un proceso continuo para mantenerse al tanto de las amenazas emergentes.
3. **Reforzar la Conectividad con Redundancia**: para garantizar la continuidad del servicio en caso de fallos o ataques, es importante implementar la redundancia en la conectividad de los sistemas críticos. Esto implica tener múltiples dispositivos

conectados mediante diferentes sistemas de comunicación, como cableado e inalámbrica. Además, se debe utilizar tecnología diversa siempre que sea posible, lo que proporciona una capa adicional de resiliencia. La redundancia de la conectividad minimiza el impacto de los ataques y los fallos en el servicio.

Medidas contra los ataques de drenaje de batería

Los ataques de drenaje de batería tienen como objetivo agotar la energía de los dispositivos IoT de manera maliciosa, lo que puede afectar seriamente su operación y vida útil. A continuación, se exponen algunas medidas correctivas fundamentales para garantizar un inicio seguro y confiable.

1. **Monitorizar el Consumo de Batería de Dispositivos Desatendidos**: la monitorización activa del consumo de batería en dispositivos IoT desatendidos es esencial para detectar posibles anomalías. Esto implica el seguimiento constante de la cantidad de energía que consumen los dispositivos en condiciones normales de funcionamiento. Cualquier aumento significativo y no justificado en el consumo de batería puede ser un indicio de un ataque de drenaje de batería en curso. Las alertas automáticas pueden ayudar a identificar estos eventos y tomar medidas preventivas.
2. **Proteger contra Ataques de Drenaje de Batería Maliciosos**: los ataques malintencionados que buscan agotar la batería de un dispositivo pueden ser devastadores. Para protegerse contra estos ataques, se deben implementar medidas de seguridad, como la detección de ataques de denegación de sueño. Esto implica establecer límites y controles para las solicitudes de red entrantes que pueden afectar el consumo de energía del dispositivo. Además, es importante asegurarse de que los dispositivos tengan mecanismos de detección de ataques y políticas de gestión de energía inteligentes que minimicen el riesgo de agotamiento de la batería debido a ataques maliciosos.

Medidas contra los ataques en el arranque

Los ataques en el arranque, que buscan comprometer la integridad del inicio de los dispositivos IoT, pueden tener consecuencias fatales para su seguridad y operatividad. A continuación, se ofrecen medidas correctivas fundamentales para proteger los dispositivos IoT contra los ataques en el arranque, garantizando así un inicio seguro y confiable en estos sistemas.

1. **Implementar Procesos de Seguridad Durante el Arranque**: es fundamental implementar procesos de seguridad robustos durante el proceso de arranque de los dispositivos IoT. Esto puede incluir la verificación de la integridad del software que se carga durante el arranque. La autenticación de los programas y procesos que forman parte de este proceso garantiza que solo se ejecuten componentes autorizados y confiables. La detección de cualquier alteración en el software durante el arranque puede indicar un posible ataque y desencadenar medidas de seguridad adicionales.
2. **Utilizar Tecnologías de Arranque Seguro**: las tecnologías de arranque seguro, como TPM (Módulo de Plataforma Confiable), son esenciales para garantizar que solo se carguen programas autorizados durante el proceso de arranque. Estas tecnologías incorporan medidas de seguridad, como firmas digitales y verificación de integridad,

para garantizar que el firmware y el software sean auténticos y no hayan sido comprometidos. Esto protege contra la ejecución de programas maliciosos durante el arranque.

3. **Limitar el Acceso Físico al Dispositivo**: restringir el acceso físico al dispositivo es una medida crítica para prevenir ataques de arranque que requieren acceso físico al hardware. Esto implica asegurar que los dispositivos IoT estén instalados en lugares seguros y que el acceso físico esté restringido a personal autorizado. El uso de carcasas resistentes a manipulaciones y otras medidas físicas de seguridad puede dificultar aún más los intentos de acceso no autorizado.

5.2 Capa de red

Medidas contra los ataques de suplantación

Los ataques de suplantación, que como ya se ha comentado en el apartado 4, se basan en el intento de aprovechar identidades falsas para tratar de realizar intrusiones no autorizadas y accesos indebidos a los dispositivos IoT. A continuación, se proporciona un listado de medidas correctivas para proteger nuestros sistemas IoT contra los ataques de suplantación en la capa de red.

1. **Implementar Medidas de Autenticación y Autorización Fuertes**: garantizar la autenticación y autorización sólidas para todos los dispositivos conectados es esencial para prevenir ataques de suplantación. Esto implica verificar la identidad de cada dispositivo antes de permitir su acceso a la red. El uso de autenticación multifactor (MFA) y técnicas de cifrado robustas asegura la integridad y la confidencialidad de los datos transmitidos y garantiza que solo los dispositivos legítimos puedan acceder a la red.

2. **Segmentación de la Red IoT en Subredes Separadas**: la segmentación de la red IoT en subredes separadas puede ayudar a limitar la propagación de un ataque de suplantación. Al dividir la red en segmentos más pequeños, se reducen las posibilidades de que un ataque se propague de un dispositivo comprometido a toda la red. Cada subred puede tener políticas de seguridad específicas y acceso controlado.

3. **Implementar Firewalls para Filtrar el Tráfico No Deseado**: los firewalls son una línea de defensa crucial contra los ataques de suplantación. Estos dispositivos pueden filtrar el tráfico no deseado y permitir solo el acceso autorizado a la red. Configurar reglas de firewall específicas y mantenerlas actualizadas es esencial para bloquear cualquier intento de suplantación.

4. **Utilizar Tecnologías de Detección de Intrusos**: las tecnologías de detección de intrusos (IDS, por sus siglas en inglés) son valiosas para identificar comportamientos anómalos en la red. Los IDS pueden alertar sobre actividades sospechosas, como intentos de suplantación o movimientos no autorizados dentro de la red. La implementación de un IDS permite una respuesta rápida a incidentes y la mitigación de amenazas antes de que causen un daño significativo.

Medidas contra los ataques de acceso no autorizado

Los ataques de acceso no autorizado buscan obtener acceso ilegítimo a dispositivos o sistemas IoT, lo que puede tener consecuencias graves en términos de privacidad y seguridad de los datos. A continuación, se expone una batería de medidas para proteger los sistemas IoT contra los ataques de acceso no autorizado.

1. **Segmentación de la Red con Elementos de Seguridad y Filtrado de Tráfico**: la segmentación de la red es una estrategia fundamental para evitar que un dispositivo infectado acceda al resto del sistema. Se deben crear segmentos lógicos que separen los dispositivos, especialmente aquellos con diferentes funcionalidades y medidas de seguridad. Implementar elementos de seguridad, como firewalls y filtrado de tráfico, entre los diferentes segmentos refuerza aún más la protección y controla el flujo de datos entre ellos.
2. **Cifrado de Datos Transmitidos y Almacenados**: el cifrado de los datos transmitidos y almacenados por los dispositivos IoT es esencial para protegerlos contra accesos no autorizados. El uso de cifrado garantiza que incluso si un atacante intercepta los datos, no podrá comprender ni utilizar la información. Esto es crucial para mantener la confidencialidad y la integridad de los datos.
3. **Supervisión Constante del Tráfico de Red**: la supervisión constante del tráfico de red en los dispositivos IoT es clave para identificar cualquier actividad sospechosa o no autorizada. Los sistemas de monitorización pueden detectar patrones anómalos y alertar sobre intrusiones o intentos de acceso no autorizado. La respuesta temprana es fundamental para prevenir posibles ataques.
4. **Asegurar la Instalación y Configuración de Dispositivos Externos**: los dispositivos IoT que estarán expuestos a Internet deben ser instalados y configurados de manera segura. Esto implica cambiar contraseñas predeterminadas, aplicar actualizaciones de seguridad, y seguir las mejores prácticas de configuración. Minimizar la superficie de ataque en estos dispositivos reduce el riesgo de que un atacante obtenga acceso a los dispositivos internos del sistema a través de ellos.
5. **Aislamiento Inmediato de Dispositivos Infectados**: en caso de que se detecte un dispositivo infectado, es fundamental aislarlo de la red de forma inmediata para evitar la propagación del malware. Esto se logra desconectando el dispositivo de la red y realizando un análisis de seguridad para comprender la naturaleza y el alcance del ataque.

Medidas contra los ataques DoS y DDoS

Los ataques DoS y DDoS tiene, como ya se ha comentado, el objetivo de agotar la capacidad de los dispositivos IoT o las redes que los conectan, lo que puede resultar en interrupciones significativas en la operación normal y el acceso a los servicios. A continuación, se expone una serie de medidas para proteger los sistemas IoT de dichos ataques.

1. **Implementar Sistemas de Detección y Mitigación Robustos**: es esencial contar con sistemas de detección y mitigación de ataques DoS/DDoS robustos que puedan identificar patrones de tráfico malicioso. Estos sistemas deben ser capaces de tomar medidas inmediatas para bloquear o mitigar el impacto de los ataques. Pueden utilizar

algoritmos de detección de anomalías, análisis de firmas y técnicas de inteligencia artificial para identificar ataques en tiempo real.

2. **Utilizar Firewalls, Sistemas de Prevención de Intrusiones y Soluciones de Mitigación en la Nube**: la protección contra ataques DoS/DDoS debe ser multicapa. Esto implica la implementación de firewalls y sistemas de prevención de intrusiones (IPS) en la red para bloquear el tráfico malicioso en el perímetro. Además, las soluciones de mitigación en la nube son útiles para hacer frente a ataques masivos que podrían saturar la infraestructura local.
3. **Diseñar Infraestructura de Red Capaz de Manejar Picos de Tráfico**: la capacidad de la infraestructura de red y los sistemas para manejar picos de tráfico inesperados es esencial para resistir los ataques DoS. Se pueden utilizar técnicas como el equilibrio de carga y la redundancia para distribuir la carga de manera eficiente entre múltiples servidores y recursos. Esto garantiza la disponibilidad continua de los servicios incluso durante un ataque.
4. **Monitorización Constante de la Red y Detección Temprana**: la monitorización constante de la red es fundamental para detectar patrones de tráfico sospechoso y responder rápidamente a los ataques. Los sistemas de alerta temprana pueden identificar aumentos repentinos en el tráfico o comportamientos inusuales y activar medidas de mitigación de manera automática. La respuesta rápida es clave para minimizar el impacto de los ataques DoS.

Medidas contra los ataques de datos en tránsito

Los ataques de datos en tránsito se centran en la interceptación o manipulación de datos mientras se transmiten entre dispositivos IoT o hacia sistemas de gestión centralizados, lo que puede comprometer la integridad y la confidencialidad de los datos. A continuación, se expone una relación de medidas para garantizar la seguridad de los datos en tránsito.

1. **Utilizar Protocolos de Comunicación Seguros**: la seguridad de los datos en tránsito es fundamental. Para protegerlos, es esencial utilizar protocolos de comunicación seguros, como el cifrado de extremo a extremo. Este cifrado garantiza que los datos estén protegidos durante todo el proceso de transmisión y recepción, lo que asegura su confidencialidad e integridad. Además, se deben implementar algoritmos de cifrado robustos y mantenerlos actualizados para resistir a las amenazas actuales.
2. **Autenticar y Autorizar Dispositivos y Entidades**: la autenticación y autorización adecuadas son cruciales para asegurarse de que solo los dispositivos y las entidades legítimas participen en el intercambio de datos. Esto se logra mediante mecanismos como certificados digitales, autenticación basada en claves o autenticación multifactor. Estas medidas garantizan que quienes acceden a los datos estén debidamente autorizados y autenticados.
3. **Segmentación de la Red para Evitar Movimiento No Autorizado de Datos**: la segmentación de la red es una medida que previene el movimiento no autorizado de datos. Al dividir la red en segmentos lógicos, se limita el acceso a los datos solo a dispositivos y entidades autorizados en cada segmento. Esto reduce el riesgo de que un

atacante que obtenga acceso a una parte de la red pueda acceder a otros segmentos sin autorización.

4. **Monitorización Constante del Tráfico de Datos**: la monitorización constante del tráfico de datos es esencial para detectar cualquier actividad sospechosa o anomalías en tiempo real. Los sistemas de detección de intrusiones y análisis de tráfico pueden identificar patrones inusuales que podrían indicar una interceptación de datos. La respuesta rápida a estas alertas es fundamental para mitigar los ataques y proteger la integridad de los datos.

Medidas contra los ataques de enrutamiento

Los ataques de enrutamiento tienen como objetivo manipular o interrumpir la ruta de comunicación entre elementos del sistema, lo que puede tener consecuencias perjudiciales para la operatividad y la seguridad de los mismos. A continuación, se aporta un listado con medidas correctivas que permiten proteger los sistemas IoT contra los ataques de enrutamiento.

1. **Implementar Protocolos de Seguridad de Enrutamiento**: utilizar protocolos de enrutamiento seguros que incorporen mecanismos de autenticación y validación de rutas. Esto asegura que solo las rutas legítimas sean utilizadas y reduce la probabilidad de sufrir modificaciones malintencionadas.
2. **Vigilancia Activa de la Red**: monitorizar de manera continua y activa la red en busca de cambios en las rutas de enrutamiento. Las soluciones de detección de anomalías pueden alertar sobre cambios inesperados en las rutas, lo que permite una respuesta temprana ante posibles ataques.
3. **Segmentación de la Red**: dividir la red IoT en segmentos lógicos separados y aplicar políticas de enrutamiento específicas para cada uno. Esto limita la propagación de rutas falsas y reduce el impacto de los ataques de enrutamiento en toda la red.

5.3 Capa de middleware

Medidas contra los ataques de signature wrapping

Los ataques de signature wrapping apuntan a manipular la verificación de firmas digitales en la capa de middleware, comprometiendo así la autenticidad e integridad de los datos y comandos transmitidos. A continuación, se expone una serie de medidas correctivas para salvaguardar nuestros sistemas IoT contra los ataques de signature wrapping.

1. **Implementar Mecanismos de Verificación de Firmas Robustos**: para prevenir ataques de signature wrapping, es fundamental contar con mecanismos de verificación de firmas robustos. Estos mecanismos deben ser capaces de detectar cualquier intento de manipulación de las firmas XML, lo que garantiza la integridad de los mensajes y evita la ejecución de acciones no autorizadas.

2. **Uso de Algoritmos de Firma Robustos y Seguros**: utilizar algoritmos de firma robustos y criptográficamente seguros es esencial para evitar vulnerabilidades conocidas y debilidades en la seguridad. Se deben seguir las mejores prácticas de criptografía y utilizar algoritmos ampliamente reconocidos y evaluados por expertos en seguridad.
3. **Mantenimiento Regular del Middleware y Actualizaciones de Seguridad**: el mantenimiento regular del middleware y sus componentes es fundamental. Se deben aplicar los últimos parches de seguridad y actualizaciones para cerrar posibles brechas de seguridad y mitigar las vulnerabilidades conocidas. Esto asegura que el middleware esté al día en términos de seguridad y protección contra amenazas emergentes.

Medidas contra los ataques de inyección SQL

Los ataques de inyección SQL tiene como objetivo explotar vulnerabilidades en las interfaces de bases de datos de dispositivos IoT, lo que puede dar lugar a la extracción no autorizada de datos o la manipulación de la información almacenada. A continuación, se ofrece un listado de medidas para proteger los sistemas IoT contra los ataques de inyección SQL.

1. **Validación y Filtrado de Entrada**: implementar técnicas de validación y filtrado de entrada para garantizar que los datos enviados al middleware sean seguros y no contengan comandos SQL maliciosos. Esto puede incluir el uso de listas blancas para permitir solo caracteres y valores específicos, listas negras para bloquear valores potencialmente peligrosos y la validación de formatos de entrada para asegurar que los datos sean coherentes con lo esperado.
2. **Consultas Parametrizadas y Preparadas**: utilizar consultas parametrizadas y preparadas en lugar de concatenar directamente datos de entrada en las consultas SQL. Estas técnicas separan claramente los datos de la consulta SQL, lo que dificulta que los atacantes puedan modificar la estructura de la consulta en ejecución. Las consultas parametrizadas también evitan la necesidad de escapar manualmente los datos, lo que reduce el riesgo de errores.
3. **Restricción de Privilegios**: asegurar que el middleware tenga los privilegios mínimos necesarios para acceder y manipular la base de datos imprescindibles para su funcionamiento. Limitar los privilegios reduce el impacto de un ataque de inyección SQL, ya que el atacante tendrá menos capacidad para realizar acciones maliciosas. Evitar el uso de cuentas de administrador en aplicaciones en vivo.

Medidas contra los ataques Man-in-the-Middle (MitM)

Los ataques Man-in-the-Middle (MitM) se basan en la interceptación de las comunicaciones por parte de un atacante, lo que puede llevar a una fuga de datos, manipulación de los mismos o suplantación de identidad. A continuación, se aportará una serie medidas correctivas cruciales para proteger nuestros sistemas IoT de este tipo de ataques.

1. **Cifrado de Extremo a Extremo**: implementar el cifrado de extremo a extremo para proteger la confidencialidad e integridad de los datos en tránsito y utilizar protocolos de seguridad sólidos, como HTTPS (para aplicaciones web) o MQTT con TLS/SSL (para

comunicaciones MQTT), que proporcionan capas adicionales de seguridad para prevenir la interceptación y modificación de datos por parte de un atacante en el medio.

2. **Autenticación Mutua**: establecer un mecanismo de autenticación mutua entre los dispositivos IoT y el middleware. Esto garantiza que solo los dispositivos y aplicaciones autorizadas puedan comunicarse entre sí. Los dispositivos deben verificar la identidad del middleware y viceversa antes de establecer una conexión.
3. **Verificación de Certificados**: verificar la autenticidad de los certificados utilizados en la comunicación entre dispositivos y el middleware y utilizar un sistema de gestión de certificados para emitir, renovar y revocar certificados de manera segura. Esto ayuda a prevenir ataques de suplantación (spoofing) y garantiza que los datos se transmitan a través de canales seguros.
4. **Sistemas de Detección de Anomalías**: implementar sistemas de detección de anomalías que monitoricen las comunicaciones en busca de patrones sospechosos o comportamientos anómalos. Estos sistemas pueden identificar posibles ataques MitM al detectar cambios inesperados en el tráfico de red o en el comportamiento de los dispositivos. Una detección temprana permite una respuesta efectiva y precisa.

5.4 Capa de gateway

Medidas contra los ataques al “secure on-boarding”

Los ataques al “secure on-boarding” se basan en comprometer el proceso seguro de incorporación de dispositivos IoT en la red a través de la capa de gateway, lo que puede dar lugar a vulnerabilidades significativas. A continuación, se ofrecerá una serie de medidas para proteger nuestros sistemas IoT contra dichos ataques.

1. **Cifrado de Extremo a Extremo**: aplicar el cifrado de extremo a extremo para garantizar la confidencialidad e integridad de los datos en tránsito durante el proceso de on-boarding. Utilizar protocolos de seguridad sólidos como HTTPS o MQTT con TLS/SSL para prevenir la interceptación y modificación de los datos por parte de un atacante en el proceso de integración.
2. **Autenticación Mutua**: establecer un mecanismo de autenticación mutua entre los dispositivos IoT y el gateway durante el proceso de on-boarding. Esto asegura que solo los dispositivos y aplicaciones autorizadas puedan comunicarse e integrarse en el sistema. Se puede lograr mediante el uso de certificados digitales o claves de autenticación conocidas de antemano para establecer una relación de confianza entre las partes.
3. **Sistemas de Detección de Anomalías**: implementar sistemas de detección de anomalías que monitoricen las comunicaciones durante el proceso de on-boarding en busca de patrones sospechosos o comportamientos anómalos. Esto permite identificar posibles ataques de intermediario y tomar acciones oportunas para proteger la integridad del sistema desde el principio.

Medidas contra los ataques a interfaces innecesarias

Los ataques a interfaces innecesarias se dirigen a interfaces de comunicación que se mantienen activas sin ser necesarias, pueden suponer un riesgo de exposición para los sistemas IoT, aumentando la superficie de ataque. A continuación, se expondrá una serie de medidas para proteger nuestros sistemas IoT contra este tipo de ataques.

1. **Evaluación de Interfaces**: realizar una evaluación exhaustiva de las interfaces presentes en el gateway para identificar aquellas que son innecesarias o no utilizadas y desactivar o eliminar estas interfaces para reducir la superficie de ataque, lo que dificulta las vías de acceso que el atacante puede usar para lograr acceso no autorizado.
2. **Configuración Segura del Gateway**: asegurar que el gateway esté configurado correctamente con medidas de seguridad adecuadas y utilizar contraseñas fuertes y actualiza regularmente el firmware del gateway para mantenerlo protegido contra vulnerabilidades conocidas.
3. **Segmentación de Red**: dividir las redes conectadas a través del gateway en segmentos lógicos. Esto puede ayudar a reducir el impacto de los ataques, ya que limita la propagación de cualquier intrusión a través de las interfaces innecesarias. También es recomendable introducir dispositivos de protección entre segmentos diferentes, como firewalls.
4. **Monitorización y Detección de Intrusiones**: desplegar sistemas de monitorización y detección de intrusiones que alerten sobre cualquier actividad sospechosa o intento de acceso no autorizado a las interfaces del gateway. La monitorización constante permite una respuesta rápida y eficiente a los ataques, lo que puede ayudar a mitigar los riesgos antes de que causen un impacto real en el sistema.

Medidas contra los ataques de extremo a extremo

Los ataques de extremo a extremo tienen como objetivo comprometer la integridad y la seguridad de todas las etapas de la comunicación y los procesos, lo que puede impactar profundamente la confiabilidad de los sistemas IoT. A continuación, se aporta una lista con medidas correctivas para proteger los sistemas contra este tipo de ataques.

1. **Selección de Protocolos de Comunicación Seguros**: elegir protocolos de comunicación para los sistemas IoT que admitan el cifrado de extremo a extremo y que no requieran la decodificación de mensajes en los gateways. Protocolos como MQTT con TLS/SSL o HTTPS son ejemplos de opciones seguras.
2. **Minimizar la Traducción de Datos en el Gateway**: reducir la necesidad de traducir información de un protocolo a otro en el gateway mediante la selección cuidadosa de dispositivos y protocolos utilizados en tu sistema IoT. Al minimizar la traducción en el gateway, se reduce la exposición de los datos descifrados y se mejora la seguridad general del sistema.
3. **Protección de los Dispositivos Gateway**: asegurar que los dispositivos gateway estén adecuadamente protegidos implementando medidas de seguridad, como la autenticación fuerte, la segmentación de redes y la monitorización constante, para proteger los gateways y reducir el riesgo de comprometer los datos descifrados en caso de un ataque.

Medidas contra los ataques a las actualizaciones de firmware

Los ataques a las actualizaciones de firmware tienen como objetivo comprometer el proceso de actualización de software en dispositivos IoT, lo que puede resultar en la implantación de versiones de firmware maliciosas o en la desactivación de medidas de seguridad. A continuación, se expone una serie de medidas para minimizar los riesgos de este tipo de ataques.

1. **Verificación de Firmas Digitales**: verificar la validez de las firmas digitales de los archivos de firmware durante el proceso de actualización de firmware. Esto garantiza la autenticidad e integridad de los archivos si se comprueba que las firmas de los archivos descargados coincidan con las firmas legítimas proporcionadas por el fabricante o el proveedor del firmware.
2. **Protección de Claves de Firma**: almacenar de manera segura las claves de firma utilizadas para verificar la autenticidad de las actualizaciones de firmware. Estas claves deben estar protegidas en el dispositivo o el gateway encargado de la descarga y aplicación de las actualizaciones. Con ello, se previenen los ataques de suplantación y se garantiza que solo las actualizaciones firmadas por una entidad de confianza sean aceptadas.
3. **Registro de Versiones de Firmware**: mantener un registro de las versiones actuales y nuevas del firmware instalado en los dispositivos IoT. Esto te permitirá verificar la integridad del firmware instalado y detectar cualquier intento de manipulación o reemplazo de firmware por parte de un atacante, lo que podría ser una señal de compromiso.
4. **Utilización de Canales de Comunicación Seguros**: emplear canales de comunicación seguros para evitar la interceptación y manipulación de los archivos de firmware durante el proceso de descarga y aplicación de actualizaciones y utilizar protocolos seguros como HTTPS, SFTP o MQTT sobre TLS para proteger la integridad y la confidencialidad de las actualizaciones de firmware. Esto asegura que las actualizaciones lleguen de manera íntegra y segura a los dispositivos IoT.

5.5 Capa de aplicación

Medidas contra los ataques de robo de información

Los ataques de robo de información buscan el acceso no autorizado y la extracción de datos críticos de dispositivos IoT, lo que puede resultar en la exposición de información confidencial y privacidad comprometida. A continuación, se ofrece una relación de medidas para minimizar este tipo de ataques en el sistema.

1. **Cifrado de Extremo a Extremo**: utilizar cifrado de extremo a extremo para proteger la confidencialidad de los datos en tránsito. Esto significa que los datos se cifran en el origen y se descifran solo en el destino final. Adicionalmente, se pueden utiliza protocolos de seguridad sólidos, como HTTPS o TLS, para garantizar que la información se transmita de manera segura y no pueda ser interceptada por atacantes mientras viaja por la red.

2. **Aislamiento y Protección de Datos Sensibles**: aislar y proteger los datos sensibles en la aplicación de IoT. Esto implica separar los datos confidenciales de otros datos menos sensibles y aplicar medidas de seguridad específicas a los datos críticos. La segmentación de red también puede ser útil para limitar el acceso a datos sensibles solo a usuarios o dispositivos autorizados.
3. **Autenticación y Autorización**: implementar métodos de autenticación y autorización para garantizar que solo actores de confianza puedan comunicarse con la aplicación y utilizar autenticación sólida para verificar la identidad de los usuarios y dispositivos antes de permitir el acceso. Además, establecer políticas de autorización que determinen qué acciones pueden realizar los usuarios autorizados en la aplicación.
4. **Auditoría y Monitorización**: establecer sistemas de auditoría y monitorización para detectar posibles actividades sospechosas o intentos de robo de información. La auditoría registra las actividades realizadas en la aplicación y permite rastrear eventos sospechosos. La monitorización constante del tráfico y la detección de patrones inusuales ayudan a identificar posibles amenazas. Estas medidas permiten una respuesta rápida ante incidentes de seguridad y la identificación de posibles vulnerabilidades en los sistemas.

Medidas contra los ataques al control de accesos

Los ataques al control de accesos tienen como objetivo eludir o comprometer los sistemas de autenticación y autorización, lo que puede resultar en accesos no autorizados a dispositivos o datos sensibles. A continuación, se ofrece una serie de medidas para proteger los sistemas IoT contra este tipo de ataques.

1. **Autenticación Fuerte**: utilizar mecanismos de autenticación fuertes, como contraseñas seguras, autenticación multifactor (MFA) o autenticación basada en certificados, para garantizar que solo los usuarios autorizados puedan acceder a los datos o cuentas en la aplicación. Esto añade una capa adicional de seguridad al verificar la identidad del usuario antes de permitir el acceso.
2. **Políticas de Autorización Granulares**: establece políticas de autorización granulares que especifiquen los niveles de acceso y los permisos para usuarios y procesos. Esto garantiza que cada usuario o proceso solo tenga acceso a los recursos necesarios y restringe cualquier acceso no autorizado. De esta manera, se limita el riesgo de que los usuarios accedan a información o funcionalidades para las que no están autorizados.
3. **Gestión de Credenciales Segura**: implementar buenas prácticas en la gestión de credenciales, como el almacenamiento seguro de contraseñas utilizando técnicas como el uso de algoritmos de “hash” (resumen) y “salt” (cadena aleatoria) para proteger las credenciales de acceso.
4. **Control de Acceso Basado en Roles**: implementar un control de acceso basado en roles para simplificar la administración de permisos y facilitar la asignación y revocación de acceso. Esto permite una gestión más eficiente de los derechos de acceso, ya que los usuarios se agrupan en roles con permisos específicos. Además, reduce el riesgo de errores humanos al definir quién tiene acceso a qué recursos.

Medidas contra los ataques de interrupción del servicio

Los ataques de interrupción del servicio buscan perturbar o bloquear deliberadamente los servicios y operaciones de los elementos de la capa de aplicación, lo que puede resultar en la pérdida de disponibilidad y funcionalidad crítica. A continuación, se expone una batería de medidas para minimizar el riesgo de estos ataques en el sistema.

1. **Firewalls y Sistemas IDS/IPS**: utilizar soluciones como firewalls y sistemas de detección y prevención de intrusos (IDS/IPS) para identificar y mitigar ataques de denegación de servicio (DoS). Estas soluciones pueden ayudar a filtrar el tráfico malicioso y detectar patrones de ataque para una respuesta temprana.
2. **Monitorización en Tiempo Real**: implementar sistemas de monitorización en tiempo real que puedan detectar patrones de tráfico anormal o comportamiento sospechoso que puedan indicar un ataque de interrupción de servicio. La monitorización constante permite identificar y responder rápidamente a los ataques.
3. **Autenticación y Autorización Robustas**: establecer mecanismos de autenticación y autorización robustos para garantizar que solo los usuarios y dispositivos autorizados puedan acceder y utilizar los servicios de la aplicación IoT. Esto evita que los atacantes interactúen con el sistema y lo sobrecarguen.
4. **Protección y Distribución de Tráfico**: utilizar sistemas de protección y distribución de tráfico de terceros que puedan proporcionar escalabilidad y capacidad adicional para hacer frente a un aumento repentino en el tráfico. Estos sistemas distribuyen la carga de manera eficiente y protegen los recursos de la aplicación contra ataques de saturación.

Medidas contra los ataques de inyección de código

Los ataques de inyección de código tienen como objetivo la inserción de código malicioso en las aplicaciones de control y visualización de datos del sistema IoT, lo que puede resultar en la ejecución de acciones no autorizadas y la toma de control no deseado. A continuación, se aporta una serie de medidas para proteger los sistemas IoT contra este tipo de ataques.

1. **Validación y Sanitización de Entradas**: aplicar controles adecuados para validar y sanitizar todas las entradas de datos recibidas en la aplicación. Esto ayudará a prevenir la ejecución de scripts maliciosos o código inyectado.
2. **Escapado de Caracteres Especiales**: implementar mecanismos de escapado adecuados para evitar la interpretación indebida de caracteres especiales en las entradas de datos. Esto reducirá el riesgo de inyección de código.
3. **Listas de Control de Acceso**: establecer listas de control de acceso (ACL) para restringir y controlar los privilegios de los usuarios en las aplicaciones, lo que limita las acciones que pueden realizar, reduciendo la superficie de ataque.
4. **Uso de Frameworks Seguros**: Utiliza frameworks y bibliotecas de desarrollo seguros que implementen controles de seguridad y validación de forma predeterminada. Estos frameworks ayudarán a prevenir vulnerabilidades comunes de inyección de código.

Medidas contra los ataques de interceptación

Los ataques de interceptación se centran en la captura no autorizada de datos en tránsito, lo que puede comprometer la confidencialidad y la integridad de la información transmitida. A continuación, se ofrece un listado de medidas para minimizar el riesgo de este tipo de ataques en el sistema.

1. **Implementar protocolos de cifrado robustos:** utilizar protocolos de cifrado sólidos, como TLS (Transport Layer Security) o HTTPS, para garantizar que los datos se transmitan de manera segura. Estos protocolos cifran los datos durante la transmisión y proporcionan autenticación para verificar la identidad del servidor, lo que evita que los atacantes puedan leer o interceptar los datos en tránsito.
2. **Utilizar técnicas de tunelización como VPN:** utilizar tecnologías como VPN (Redes Privadas Virtuales), que establecen conexiones seguras a través de redes públicas, como Internet, creando un "túnel" cifrado para el tráfico de datos. Esto dificulta la interceptación de datos por parte de terceros, ya que incluso si un atacante logra interceptar el tráfico, solo verá datos cifrados difíciles de descifrar sin la clave adecuada.
3. **Establecer mecanismos sólidos de autenticación y autorización:** establecer mecanismos efectivos de autenticación y autorización para determinar qué entidades tienen acceso a los sistemas y cuál es su nivel de permisos una vez se otorga el acceso. Esto evita que los atacantes obtengan acceso no autorizado a los datos y recursos de la aplicación. Las medidas pueden incluir contraseñas seguras, autenticación de dos factores y políticas de acceso basadas en roles.

6 Método de Aplicación

A la hora de realizar el análisis de las amenazas y proponer medidas correctivas para las mismas en los casos de estudio que se analizarán a continuación, se va a utilizar una metodología de desarrollo propio basada en la combinación de diversas metodologías, marcos y estándares de seguridad del ámbito de la ciberseguridad, lo que permite abordar de manera eficaz la identificación, evaluación y mitigación de amenazas en sistemas IoT. Cada uno de estos enfoques aporta fortalezas específicas que se aprovecharán para desarrollar esta metodología integral.

El primer paso a la hora de analizar los casos será la identificación del contexto y la naturaleza del sistema analizado utilizando principios y conceptos desarrollados por la normativa ISO 27001. Dicho contexto, el tipo de información y la criticidad de la misma serán elementos clave a la hora de evaluar a qué amenazas están expuestos y qué nivel de exigencia en cuanto a medidas de seguridad plantea. Según esta metodología, los sistemas podrán categorizarse en tres tipos dependiendo del nivel de seguridad que requieran teniendo en cuenta la naturaleza de los datos que manejan. Los niveles quedarían de la siguiente forma:

- Nivel bajo: procesa datos a los que no se aplica ningún tipo de normativa de privacidad y no tiene ningún impacto sobre el mundo físico.
- Nivel medio: procesa datos de los cuales se puede extraer información relacionada con usuarios o elementos del sistema, como ubicaciones o direcciones IP. Pueden tener impacto en el mundo físico, pero con baja o nula probabilidad de provocar daños al medio ambiente o sobre la vida humana.
- Nivel alto: procesa datos entre los cuales se incluyen datos sensibles (datos que permiten identificar al usuario que los genera). Tienen impacto en el mundo físico y probabilidad de causar daños en el medio ambiente o sobre la vida humana.

Una vez hecho esto, el siguiente paso será analizar el diseño de cada una de las capas, la funcionalidad y requisitos que deben cumplir, los elementos que las integrarán y las amenazas a las que deberán responder. Para este análisis, se utilizarán las amenazas del apartado 4. Con todo ello, se podrá ofrecer una relación detallada de las amenazas de cada capa y su impacto en el sistema.

Después de revisar las amenazas y su impacto en el sistema, se procederá a ofrecer una serie de medidas adaptadas al caso de estudio, de forma que su aplicación permita minimizar o eliminar el riesgo (según sea el caso). Estas medidas estarán recopiladas y extraídas de los controles de las normativas, frameworks y guías mencionadas en el apartado 4 para cada una de las amenazas.

Tanto las amenazas potenciales a analizar como la cantidad de medidas correctivas y la complejidad de las mismas vendrán dadas por los requerimientos de seguridad del sistema. Dichos requerimientos están, a su vez, directamente relacionados con el grado de confidencialidad de los datos que maneja y la afectación que puede producir el sistema en aspectos determinantes para el mundo físico, como por ejemplo la seguridad de las personas. De esta forma se asegura que no se exijan el mismo nivel de seguridad a un sistema de visualización de datos de humedad en una planta agrícola que a un sistema de monitorización de datos de tráfico.

A continuación, se muestra un diagrama con el planteamiento descrito:

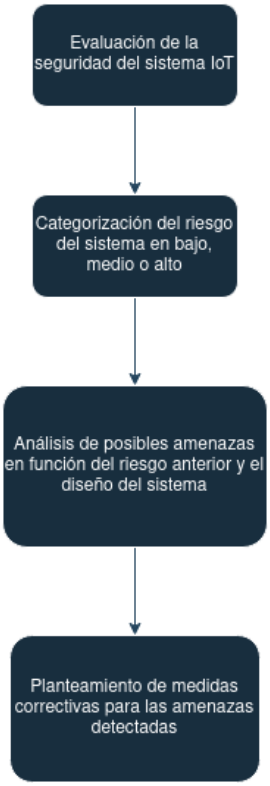

Figura 2: diagrama de la metodología planteada.

Esta metodología integrada aprovecha la fortaleza de los marcos y estándares reconocidos para ofrecer una estrategia completa y basada en las mejores prácticas de la industria. Por tanto, el lector tendrá una visión completa del tipo de amenazas a las que debe hacer frente un sistema IoT, el impacto que puede causar en el sistema cada una de las mismas y las posibles medidas a aplicar para el sistema estudiado.

7 Casos de estudio

Después de definir los elementos del sistema IoT, categorizar las diferentes secciones y realizar el análisis de los potenciales riesgos que pueden sufrir, es el momento de utilizar dos casos de estudio para ejemplificar de forma más concreta qué elementos pueden integrar este tipo de sistemas.

En este caso se va a evaluar qué riesgos pueden tener, tanto para cada uno de los elementos que conforman el sistema IoT como del conjunto en general, qué aspectos habría que tener en cuenta a la hora de evaluar la seguridad del sistema y algunas medidas específicas a aplicar para minimizar el riesgo eligiendo algunas tecnologías concretas, de forma que se puedan utilizar como ejemplo para extrapolarlas a cualquier otra tecnología existente utilizando las modificaciones oportunas.

Para ello, se van a definir los casos de estudio con un esquema de los elementos que lo integrarían. A continuación, se realizará un clasificación de dichos elementos en las categorías utilizadas en el apartado 3. Una vez hecho esto, se analizarán las amenazas que suponen un mayor riesgo para el caso de estudio concreto debido al diseño y la naturaleza del sistema. Por último, se planteará una tecnología con la que se podría implementar y desplegar el diseño, y se propondrán soluciones específicas utilizando dicha tecnología para minimizar los riesgos identificados en el análisis de amenazas. Este procedimiento está descrito en el apartado 6.

Con todo ello, se podrá obtener una idea general sobre los riesgos de este tipo de sistemas, las implicaciones que pueden tener en caso de no aplicar las medidas de seguridad necesarias, así como unas conclusiones generales sobre qué componentes del sistema son primordiales para la seguridad y qué elementos hay que priorizar en caso de no disponer de recursos para aplicar todas las medidas necesarias, ofreciendo un nivel de seguridad aceptable en entornos que no requieran niveles de seguridad específicos por causas legales o operacionales.

Es necesario también aclarar que en este trabajo se excluye el desarrollo del código necesario de cada uno de los elementos del sistema, así como el despliegue y configuración de los mismos, quedando fuera del ámbito del trabajo todas las acciones necesarias para lograr un sistema funcional más allá del diseño y análisis del mismo. Aunque es cierto que en algunos puntos del análisis puede ser necesario mencionar conceptos propios del desarrollo de código o configuraciones concretas de diversos elementos o del despliegue de estos, todo ello se proporciona desde una dimensión teórica y para ilustrar cómo se plasmarían las medidas planteadas en un sistema real. Dichas medidas deberían adaptarse para el sistema real implementado, siendo responsabilidad del usuario que realiza el proyecto en cada caso realizar los ajustes y pruebas para que funcionen eficientemente en el sistema en cuestión.

Tampoco será objeto del trabajo detallar la funcionalidad del sistema ni todas las interacciones entre los diferentes elementos del mismo, más allá de lo necesario para definir los requisitos de seguridad y poder hacer un planteamiento correcto para el mismo, quedando fuera cualquier aspecto que no esté directamente relacionado con el diseño y análisis del mismo.

7.1 Smart Home (Vivienda inteligente)

El primer caso de estudio se realiza sobre uno de los sistemas más comunes que se plantean a la hora de iniciarse en el mundo del IoT, pero que ofrece una base suficiente para el análisis objeto de este trabajo. El caso tratará sobre un sistema de hogar inteligente ("Smart Home") para domotizar un hogar corriente con los elementos ya existentes (domicilio con conexión a Internet mediante fibra óptica contratada con un ISP y el router proporcionado por el mismo) y una pequeña inversión.

Para ello, se va a utilizar un diseño con elementos de bajo coste en la **capa de sensorización**. En este caso, se van a utilizar tanto elementos de recolección de datos como de actuación, con el fin de no extender excesivamente el caso. Con ello, sería posible escalar el sistema para añadir más elementos de forma sencilla, ya que los principios utilizados y los análisis realizados serían igualmente aplicables con más elementos. Los dispositivos desplegados serán de tipo Arduino o compatible con la plataforma, de modo que se podrán utilizar los entornos de desarrollo y todo el conjunto de lenguajes de programación y librerías disponible para dicha plataforma, de modo que la programación se simplifica en gran medida dada la cantidad de software disponible gracias a la comunidad. En este entorno se incluye, por supuesto, librerías testeadas y securizadas para la interconexión de los dispositivos con el resto de elementos del sistema, lo que ofrece una primera capa de seguridad importante.

Para la **capa de red y gateway** se va a utilizar como base la infraestructura que un usuario pueda tener disponible. En este caso, se asume que cuenta con una red Wi-Fi doméstica y un computador de sobremesa, pudiendo añadir elementos para conformar una red independiente en caso necesario y un router para la red principal con la red de dispositivos IoT, que realizará las funciones de gateway. Estas dos capas se pueden aunar en cuanto a elementos se refiere, ya que en un caso de este tipo, donde las necesidades de conectividad no implicar restricciones demasiado estrictas ni se integran sistemas muy complejos, es preferible la simplicidad. Esto no implica un problema a la hora de analizar los requisitos a aplicar, puesto que conceptualmente es posible dividir las necesidades a pesar de que las funciones las realice un solo dispositivo o varios en conjunto.

La **capa de middleware** estará formada por un único elemento, que será el servidor de mensajería o broker MQTT. Dicho elemento será el que se encargue de la comunicación entre la capa de sensorización y la capa de aplicación, de forma que la información pueda ser generada y consumida por cada una de las capas que interconecta en función de las necesidades del sistema. Así pues, dado que es un sistema a pequeña escala y las necesidades quedan cubiertas, no será necesario añadir ningún elemento más a dicha capa.

En cuanto a la **capa de aplicación**, el usuario utilizará una solución cloud desarrollada desde cero, configurando y programando todos los elementos de dicha infraestructura, que ofrezca tanto panel web como aplicación móvil para interactuar con el sistema. La interacción incluirá tanto lectura de datos como actuación sobre elementos. Para dicha solución, se utilizará un servicio cloud que permita interconectar varios elementos, como una aplicación web y una base de datos en la que se mantenga un estado del sistema para poder visualizarlo en cualquier momento. Además, ofrecerá una interfaz API para poder realizar mediante una aplicación móvil las mismas acciones que se puedan realizar utilizando la aplicación web mencionada. El proveedor cloud elegido para este caso es Microsoft Azure[14].

14 https://azure.microsoft.com/es-es

Dicho sistema se enmarcaría en el **Nivel Bajo de requisitos de seguridad** de la metodología expuesta en el apartado 6, por lo que las medidas necesarias para el mismo se centrarán en conseguir un nivel de seguridad suficiente para cumplir unos requisitos mínimos.

Así pues, vamos a comenzar con una imagen en la que se especifica el diseño del sistema, de forma que se pueda clarificar el mismo para que sea más sencillo identificar los componentes del sistema y relacionarlos con las categorías de la clasificación del apartado 3.1.

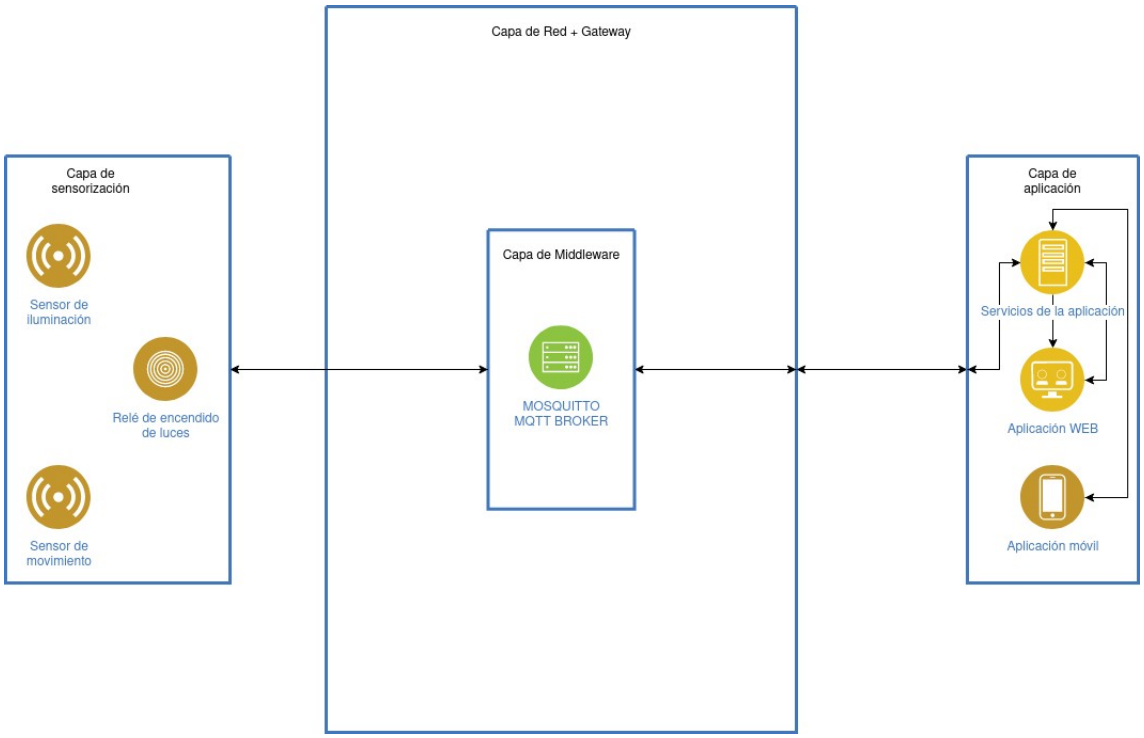

Figura 3: esquema de diseño del sistema IoT domótico planteado

7.1.1 Capa de sensorización

Para los elementos que conforman la capa de sensorización, en este caso debemos tener en cuenta ciertos condicionantes que mitigan y/o eliminan varios riesgos. Se debe tener en cuenta, como se ha mencionado en el caso de estudio, que es un sistema domótico, por lo que el acceso a la capa de sensorización queda limitado al contexto de la vivienda donde se va a realizar el despliegue de los dispositivos. Por tanto, los ataques de acceso físico a dichos sensores y actuadores se limita hasta el punto de hacerse despreciables.

En este caso, únicamente deberíamos centrarnos en los ataques que se pueden llevar a cabo sobre los dispositivos de dicha capa de forma remota, debido a que son los que más probabilidades de tener éxito tienen. En consecuencia, como se ha comentado, los ataques que se basan en tener acceso físico al dispositivo quedan relegados a un plano secundario,

asumiendo que es tan improbable el hecho de que sea viable llevarlos a cabo que pueden ser excluidos del análisis.

Por este motivo, las medidas de seguridad aplicables a la capa de sensorización en este caso de estudio se basarán en tratar de identificar los dispositivos que participan en la comunicación y que los datos que viajan entre los diferentes elementos del sistema no sean modificados antes de llegar a su destino (tanto información utilizada por el sistema como datos de de control y actualización de los dispositivos).

Entre los ataques que se podrían llevar a cabo después de realizar el descarte inicial, se encuentra el **ataque de captura de nodo**. Dicho ataque, teniendo en cuenta el sistema planteado, podría realizarse utilizando mecanismos de comunicación remota. Por tanto, este tipo de ataques podrían mitigarse en esta fase comprobando el origen de los datos, tanto de los datos de operación como de actualización y gestión. Esto podría llevarse a cabo mediante certificados autofirmados, asegurando que tanto los orígenes como los destinos de los datos mantienen una relación de confianza y validan su identidad entre ellos. Se podría utilizar una herramienta criptográfica como OpenSSL[15] para crear todos los elementos que conforman la cadena de confianza utilizada por los sistemas de criptografía de clave pública. Una vez realizado esto, se deben configurar los dispositivos para que utilicen los certificados generados para las conexiones de red, realizando la comunicación con otros elementos mediante conexiones cifradas.

En el caso concreto de estudio, en el que los elementos de la capa de sensorización se conectarían a un broker MQTT (servidor de mensajería) para transmitir los datos que recopilan y recibir actualizaciones del estado del mismo. Los diferentes sensores y actuadores se configurarán con un certificado específico para cada uno de ellos y utilizarán un nombre para la conexión con el broker. De esta forma todos los elementos serán identificables y se respetará la integridad y la confidencialidad de la información.

Utilizar una red separada para sensores, sobre todo si la comunicación se establece mediante la misma tecnología que otros equipos en un entorno compartido. Este es el caso que suele ser más común en sistemas domóticos, debido a que los dispositivos IoT se conectan a la red doméstica a través de módulos con capacidades de conectividad Wi-Fi, ya sean integrados en el propio dispositivo o externos al mismo conectados mediante entrada/salida digital o analógica. Para ello, bastaría con utilizar redes independientes a las utilizadas por los equipos de usuario domésticos, como ordenadores portátiles, tabletas, smartphones, etc. Se podría desplegar una red independiente utilizando electrónica de red separada o, para evitar costes, utilizar las redes de invitados de las que la mayor parte de equipos de proveedores de Internet disponen.

De esta forma, al utilizar una red diferente con un direccionamiento distinto, conseguimos aislar los dispositivos del resto de equipos de la red IT doméstica. Una vez hecho esto, podemos conectar el equipo que hará de servidor a dicha red mediante una interfaz específica para poder comunicarnos con los equipos IoT, o habilitar en el router/switch del operador que lo permita, un enrutamiento para que desde la red IT algunos equipos concretos puedan conectarse al direccionamiento de la red IoT. Dicha configuración se hará conforme a la especificación que marque el software y hardware de comunicación del dispositivo IoT. Para disponer de conectividad entre los dispositivos IoT y el o los equipos IT necesarios para el funcionamiento del sistema se valorará, como se ha comentado, entre configurar un enrutamiento entre la red principal IT y la red IoT para dispositivos concretos, o hacer uso de una infraestructura

15 https://www.openssl.org/

independiente. La única comunicación necesaria se realiza entre los dispositivos y el servidor de mensajería, que en este caso sería el broker MQTT.

Para asegurar una protección integral del sistema IoT, también es fundamental añadir monitorización de red para garantizar la seguridad y estabilidad de la infraestructura. La monitorización de red permite supervisar constantemente el tráfico de datos y detectar posibles anomalías o actividades sospechosas en tiempo real.

Mediante el uso de pfSense[16] como herramienta centralizada de seguridad, se pueden configurar sistemas de monitorización y registro de eventos detallados para analizar el tráfico de red en profundidad. La funcionalidad de registro de pfSense permite almacenar eventos de forma segura, lo que facilita el análisis forense y la identificación temprana de posibles intrusiones o brechas de seguridad.

Además, pfSense ofrece funcionalidades de IDS/IPS, lo que significa que no solo monitorizará el tráfico, sino que también podrá identificar y prevenir intentos de acceso no autorizados o comportamientos maliciosos en la red. Esto es especialmente valioso en un entorno IoT, donde los dispositivos integran un nivel de seguridad menor que el resto de dispositivos de red, debido a las limitaciones que tienen a causa de sus bajos recursos (por norma general)

Al integrar la monitorización de red con pfSense, se puede supervisar tanto el tráfico cifrado como el no cifrado, lo que proporciona una visión completa del tráfico tanto de entrada como de salida de esta capa. Los certificados previamente configurados en los sensores y actuadores garantizan que todas las conexiones sean seguras y confiables, lo que mejora aún más la protección.

Utilizando todas las capacidades mencionadas de la herramienta de monitorización se asegura que cualquier actividad sospechosa sea rápidamente detectada y contenida. Al mantener un registro detallado de los eventos de la red, se facilita el análisis del tráfico, lo que puede permitir analizar patrones y lineas de comportamiento del mismo, con lo que se pueden tomar medidas preventivas adaptadas al sistema en concreto para fortalecer aún más la seguridad del sistema IoT.

Medidas adicionales

Por último, una medida interesante a añadir es la redundancia de dispositivos mediante diferentes protocolos y/o tecnologías de comunicación. Una de las opciones más efectivas sería utilizar tecnologías que utilicen medios de transmisión diferentes, como inalámbricos y cableados. Esto aporta robustez al sistema ya que contamos con dos formas diferentes de transmitir la información, lo que aplicado al caso de Ethernet para la comunicación cableada y Wi-Fi para la inalámbrica aseguran que si alguno de los mecanismos falla, el otro sigue teniendo una muy alta probabilidad de poder funcionar al utilizar una tecnología radicalmente diferente. Un caso similar podría ser utilizar Wi-Fi con otra tecnología inalámbrica, aunque en este caso al ser las dos inalámbricas cabe el riesgo de que ambas se vean afectadas, por ejemplo al sufrir un ataque por interferencia de señales. Aunque es cierto que es un ataque complejo porque operan en bandas de frecuencia distintas y sistemas diferentes, sería mucho más sencillo atacar tecnologías inalámbricas que la conexión cableada.

16 https://www.pfsense.org/

7.1.2 Capa de red

Para salvaguardar eficazmente la capa de red en sistemas IoT y mitigar los riesgos asociados a los ataques, se requiere una estrategia de protección minuciosa de la red a todos los niveles, ya que es una pieza clave del mismo.

En el caso de estudio que nos ocupa, los ataques que se podrían materializar a través de esta capa son más limitados, ya que los dispositivos del sistema y los elementos de interconexión están en un entorno controlado. Por ello, las medidas de protección se basarán sobre todo en controlar el acceso a la red, analizar y responder a comportamientos anómalos o malintencionados sobre la misma y mantener los diferentes elementos que se conectan lo más aislados posible permitiendo la funcionalidad del sistema.

Una de las tácticas fundamentales para lograrlo implica la implementación de mecanismos de control y monitorización en todos los estamentos que la conforman. Esta situación es especialmente común en entornos de domótica, donde los dispositivos IoT se integran a la red doméstica mediante módulos de conectividad Wi-Fi. Para contrarrestar el riesgo que ello implica, se propone la creación de redes independientes, segregadas de los dispositivos de uso cotidiano, como computadoras portátiles, tablets y smartphones. Esto se puede lograr a través de redes de invitados, comúnmente disponibles en los routers proporcionados por los proveedores de Internet, o mediante la implementación de infraestructura de red dedicada, que sería la solución más efectiva.

Al establecer una red independiente, se logra un aislamiento efectivo de los dispositivos IoT respecto al resto de la infraestructura de la red doméstica. Para asegurar la conectividad necesaria, es posible habilitar rutas de comunicación específicas entre la red IoT y la red principal IT, a través de routers. La configuración precisa se determinará de acuerdo con las especificaciones del software y hardware de los dispositivos IoT. En un escenario donde la comunicación es esencialmente entre los dispositivos y un servidor de mensajería, como el broker MQTT, esta separación de redes garantiza que cualquier actividad maliciosa o potencialmente dañina en la red IoT se mantenga aislada, preservando la integridad y confidencialidad de la información. Como añadido a la segmentación, se puede incluir un elemento de filtrado de tráfico (o firewall) para que únicamente se puedan comunicar los elementos imprescindibles en los segmentos sensibles. La herramienta pfSense ofrece capacidades de filtrado de tráfico, lo que la posiciona como una de las mejores soluciones para este fin.

Sin embargo, como se ha dicho, asegurar la capa de red va más allá de la segmentación. Para fortalecer aún más la protección de los sistemas IoT, se sugiere implementar medidas de monitorización de red utilizando herramientas especializadas como el mencionado en la sección anterior, pfSense. Como se ha comentado, este software robusto permite configurar sistemas de registro y análisis de eventos de red, proporcionando una visión integral del tráfico intercambiado entre los dispositivos IoT y otros componentes. La funcionalidad de registro seguro y la capacidad de detectar intrusiones y comportamientos anómalos son particularmente valiosas en un entorno IoT.

Con la integración de pfSense como elemento central de monitorización y control del tráfico de red, se establece una defensa activa contra amenazas potenciales. La capacidad de supervisar tanto el tráfico cifrado como no cifrado ofrece una visión completa de la actividad de la red IoT,

y la utilización de certificados preconfigurados en los elementos del sistema asegura conexiones seguras y confiables.

La combinación de segmentación de red, monitorización de tráfico y la potencia de herramientas como la mencionada aquí establece un enfoque sólido para mitigar los riesgos de seguridad en la capa de red de los sistemas IoT.

Medidas adicionales

Por otro lado, y a pesar de que su despliegue en una red doméstica puede antojarse complejo y costoso, la implantación de un sistema de autenticación basada en certificados en una red Wi-Fi es una medida sólida para fortalecer la seguridad y garantizar la autenticidad de los dispositivos conectados. Esta estrategia se basa en el uso de certificados digitales únicos asignados a cada dispositivo, validando dichos certificados antes de conceder acceso a la red. Al requerir que los dispositivos demuestren su identidad antes de acceder a la red es mucho menos probable que un elemento malintencionado o no controlado obtenga acceso a la red. Esto reduce significativamente el riesgo de acceso no autorizado y ataques de suplantación. Además, al requerir una identificación única para cada dispositivo, se facilita la gestión y control de los dispositivos que operan en la red y es más fácil mantener un registro de trazabilidad del origen y el destino de los datos, para analizar el origen si un ataque puede materializarse.

7.1.3 Capa de middleware

En el contexto de sistemas IoT, la protección de la capa de middleware se vuelve primordial para prevenir ataques que puedan comprometer la seguridad y el funcionamiento del sistema en su conjunto, siendo el componente primario a proteger en este caso de estudio el servidor de comunicaciones, también llamado broker, que se encuentra entre los elementos de la capa de sensorización y el resto del sistema. En este caso, la tecnología utilizada sería Mosquitto[17], una solución “open source” que implementa el protocolo de mensajería MQTT.

Ante esta configuración se presentan desafíos significativos, como los **ataques de inyección SQL**, que representan una preocupación crítica al permitir que los atacantes inserten comandos maliciosos en las consultas de bases de datos, poniendo en riesgo la integridad y confidencialidad de los datos. Se sugiere una estrategia de defensa que involucra la validación estricta de entradas, el uso de sentencias parametrizadas y la normalización de datos antes de la ejecución de consultas SQL, ya que a pesar de que Mosquitto no maneja directamente bases de datos, la aplicación de medidas de seguridad a nivel de aplicación ayudará a prevenir posibles inyecciones de código malicioso.

La **interceptación y manipulación de mensajes o MitM**, también deben ser contrarrestados. Una solución efectiva ante este tipo de ataques es habilitar el cifrado de extremo a extremo en la comunicación entre dispositivos y el broker de mensajería para asegurar la privacidad y la integridad de los datos en tránsito.

17 https://mosquitto.org/

Los riesgos de **fuga de información** plantean una amenaza a la confidencialidad y privacidad de los datos. Para mitigar este riesgo, se recomienda la aplicación de controles de acceso sólidos y autenticación confiable en el middleware, limitando el acceso a datos sensibles. En Mosquitto, se deberá utilizar autenticación basada en certificados y autorización basada en ACL (Access Control Lists) para controlar el acceso de dispositivos y aplicaciones a los temas MQTT específicos. Para ello, se debe generar una lista de los temas o "topics" sobre los que los elementos pueden leer y escribir, preferiblemente configurando listas de acceso permitido (también conocidas como listas blancas) para que los elementos no incluidos en dichas listas no puedan llevar a cabo acciones en el broker de mensajería. De este modo, si un elemento externo quiere registrarse en el broker para leer o publicar mensajes, dicho mecanismo le denegará el acceso al no estar registrado, haciendo mucho más complejo un ataque por suplantación de dispositivo.

Aunque en el análisis de amenazas de la clasificación del apartado 3 no se ha incluido específicamente, la capa de middleware también puede ser blanco de **ataques de denegación de servicio (DoS)** dado que expone sus servicios en la red. Para prevenir esta situación en este caso concreto, dado que el broker de mensajería (Mosquitto) incluye configuración específica para hacerlo, se aconseja configurar límites de tasa de mensajes y conexiones en el middleware utilizando los parámetros pertinentes para restringir el número de conexiones y mensajes por segundo, asegurando una distribución equitativa de dichos recursos.

La habilitación de autenticación basada en certificados, la implementación de cifrado SSL/TLS y la configuración de límites de tráfico en Mosquitto contribuirán a la mitigación efectiva de riesgos y la creación de un entorno seguro para la capa de middleware en sistemas IoT. Mantenerse actualizado con las últimas versiones y parches de seguridad de Mosquitto también es fundamental para garantizar una defensa continua contra amenazas emergentes.

7.1.4 Capa de gateway

Asegurar la capa de gateway en sistemas IoT se vuelve de máxima importancia para contrarrestar distintos tipos de ataques que pueden comprometer la seguridad de las comunicaciones entre los dispositivos IoT y el resto de componentes del sistema.

Se presenta el desafío de prevenir **ataques al cifrado de extremo a extremo**, los cuales podrían exponer la confidencialidad de los datos transmitidos entre dispositivos y la nube. Para abordar esta inquietud, se debe adoptar una solución de cifrado SSL/TLS en el equipo que funciona como gateway, garantizando que los datos permanezcan protegidos durante su travesía y evitando posibles intentos de interceptación no autorizada. Para ello, es esencial aplicar medidas de seguridad adecuadas en el contexto de la conexión con la infraestructura en la nube de Azure. El uso de conexiones VPN al entorno de Azure mediante las soluciones del proveedor asegura una comunicación segura y directa entre el equipo gateway y las aplicaciones en la nube. Configurar políticas de seguridad y grupos de seguridad en Azure también resulta fundamental para controlar el tráfico y prevenir posibles ataques.

La eliminación de **interfaces innecesarias** se posiciona como una medida clave para mitigar riesgos. La presencia de interfaces o endpoints no utilizados podría servir de punto de entrada a atacantes. En este sentido, se aconseja deshabilitar o asegurar debidamente estas interfaces para

disminuir la superficie de ataque y evitar posibles intrusiones. Añadir un firewall que permita únicamente el tráfico de red con los servicios que se utilicen añade una capa extra de seguridad, ya que asegura únicamente tráfico de red a las interfaces deseadas.

El **secure on-boarding** de dispositivos en el sistema es otro aspecto crítico a considerar en la capa de gateway. Ataques pueden tener como objetivo el proceso de incorporación segura de dispositivos, aprovechando posibles debilidades. Para prevenir esta amenaza, es necesario establecer un proceso de autenticación riguroso y validación de dispositivos, asegurando que solo dispositivos legítimos y confiables puedan integrarse en el sistema. El uso de las políticas y roles del proveedor cloud pueden ser un mecanismo muy efectivo para evitar que elementos externos se conecten al sistema, forzando únicamente orígenes conocidos. También es un factor clave en este aspecto que todos los elementos que ingresen al sistema cuenten con certificados emitidos por una entidad de certificación conocida, o mejor incluso por la entidad utilizada para generar los certificados autofirmados del resto de elementos del sistema, de forma que todos los certificados necesarios para operar en el sistema sean creados manualmente por el administrador el sistema IoT o el actor designado por el mismo para tal fin.

Como complemento al resto de medidas en esta capa, la implementación de una estrategia de monitorización y registro de eventos en la capa de gateway, con herramientas de monitorización como pfSense (ya mencionada en otras capas) permite la detección temprana de anomalías y actividades maliciosas, así como ofrecer trazabilidad en una posible investigación del incidente en caso de que se produzca y sea necesario generar un informe pericial para identificar a los responsables del mismo.

7.1.5 Capa de aplicación

Salvaguardar la capa de aplicación en sistemas IoT es esencial para prevenir una serie de ataques que podrían comprometer la integridad y seguridad de las operaciones. Entre las amenazas a considerar se encuentran los **ataques de robo de datos**, que buscan acceder de manera no autorizada a información sensible. Para contrarrestar este riesgo, es fundamental implementar medidas de autenticación sólida y cifrado de datos en la capa de aplicación, asegurando que solo los usuarios autorizados puedan acceder a la información y que los datos se mantengan confidenciales durante la transmisión. Esto podría asegurarse al utilizar las herramientas de control de acceso y seguridad de Azure, como Azure Active Directory (Azure AD) para gestionar la autenticación y autorización de usuarios. Además, es posible utilizar Azure Key Vault permite almacenar y gestionar de manera segura las claves de cifrado y tokens de acceso de los usuarios y aplicaciones que conforman el sistema.

Los **ataques sobre el control de accesos** representan otro desafío significativo. Los atacantes podrían intentar eludir las medidas de seguridad para obtener acceso no autorizado a funciones y datos del sistema. Una solución recomendada es establecer políticas de control de acceso granular en la capa de aplicación, garantizando que los usuarios solo tengan acceso a las áreas y funciones necesarias para sus roles específicos. La herramienta mencionada anteriormente, Azure Active Directory (Azure AD) permite aplicar y gestionar el control de los elementos del sistema a otros elementos utilizando estos roles para definir qué acciones y sobre qué elementos ejecutan dichas acciones los diferentes elementos del sistema. El desarrollo de las aplicaciones

tanto web como Android debe hacer uso de dicho mecanismos para asegurar la identidad y los permisos del usuario que trata de acceder.

La **interrupción del servicio** es otra amenaza crítica a considerar. Los ataques que buscan interrumpir los servicios pueden causar una interrupción en las operaciones y afectar la disponibilidad del sistema. Para mitigar este riesgo, se sugiere implementar redundancia y escalabilidad en la infraestructura de la capa de aplicación, asegurando que haya planes de contingencia para mantener la disponibilidad en caso de un ataque exitoso. Para utilizar la escalabilidad y disponibilidad de Azure, el diseño deberá utilizar las características de alta disponibilidad y elasticidad del proveedor, desplegando la aplicación en diferentes zonas geográficas y distribuyendo la carga a los equipos que ofrezcan mejor respuesta. En el caso del proveedor seleccionado, es posible realizar esto mediante la configuración de conjuntos de recursos replicados (“availability sets”) de forma que el servicio pueda seguir operando en caso de caída de los recursos primarios que operan

Los **ataques de inyección de código** también representan una preocupación importante. Los atacantes podrían intentar insertar código malicioso en la capa de aplicación para comprometer su funcionalidad y seguridad. Una medida clave para prevenir esto es la validación y el filtrado riguroso de las entradas de usuario en la capa de aplicación, evitando la ejecución de código no autorizado. Azure Web Application Firewall (WAF) es una herramienta esencial para proteger contra ataques de inyección de código, ya que detecta y bloquea patrones de tráfico malicioso, como intentos de inyección SQL o ataques de “cross-site scripting” (XSS). En la parte de la aplicación web, también sería necesario implementar medidas de parametrización y filtrado en los campos de introducción de texto, de modo que si un atacante tiene acceso a alguna funcionalidad de la aplicación, no sea capaz de interactuar con el resto de elementos de la mismo introduciendo fragmentos de código maliciosos. En la parte de la aplicación Android, también sería deseable implementar dichos controles. De igual modo, siempre es recomendable realizar una sanitización de las entradas, de forma que se valide que la información tratada en la parte del servidor es segura y no incluye ningún tipo de inyección que pueda desembocar en un impacto en la seguridad del sistema.

Por último, la **interceptación de datos en la capa de aplicación** es una amenaza seria que podría exponer información confidencial. Para mitigar este riesgo, es esencial implementar cifrado en la transmisión de datos sensibles entre los dispositivos IoT y la capa de aplicación. Utilizar protocolos seguros como HTTPS y TLS garantiza que los datos estén protegidos durante su tránsito y no sean accesibles para atacantes. El proveedor ofrece muchas facilidades para la utilización de certificados en las aplicaciones.

En conjunto, la implementación de medidas de autenticación, control de acceso, redundancia, validación de entradas y cifrado en la capa de aplicación contribuye a fortalecer la seguridad y proteger contra una variedad de ataques en sistemas IoT. Estas estrategias permiten crear un entorno seguro y confiable en la capa de aplicación, asegurando que los datos y las operaciones se mantengan protegidos en todo momento.

7.2 Smart City (Ciudad inteligente)

En el siguiente caso de estudio, se va a analizar es un sistema de ciudad inteligente (“Smart City”) teórico similar al que podría plantearse para cualquier ciudad que pretenda realizar una implantación de estas características. Como el concepto “Smart City” es muy amplio, ya que puede abarcar una gran extensión de tipos diferentes de aplicaciones de la IoT en las ciudades, el caso de estudio se va a enfocar sobre la gestión inteligente y automatizada del tráfico. Este tipo de sistemas conllevan grandes desafíos, ya que debido a las dimensiones del sistema, el tipo de datos que manejan y la criticidad del propio sistemas implican una gestión de la seguridad el mismo a un grado de profundidad mayor.

Por tanto, en este caso, el objetivo será aplicar la cantidad de medidas que sean necesarias para asegurar el funcionamiento óptimo y en condiciones de seguridad del propio sistema. Si bien no será posible desarrollar con tanta profundidad medidas específicas para las tecnologías utilizadas, ya que es mucho más complejo definir de forma teórica cuáles deberían ser dichas tecnologías, el caso servirá para profundizar en las amenazas que pueden sufrir y presentar sistemas de protección más avanzados, que en el caso de estudio anterior serían inviables de utilizar debido a la naturaleza y planteamiento del mismo.

Así pues, y debido a la mencionada complejidad del sistema IoT planteado, el diseño del mismo se va a realizar grosso modo utilizando la categorización por capas empleada a lo largo del trabajo, pero sin entrar en detalle sobre los elementos que conformarán cada una de estas capas debido a que se añadiría excesiva información que podría desviar la atención del objeto de estudio, que es el análisis de seguridad del mismo, para lo que con tratar el diseño de forma contextual es suficiente.

Para la **capa de sensorización** se deben utilizar sensores y actuadores certificados o validados que garanticen el funcionamiento y los valores obtenidos de los mismos (para sensores) o la ejecución de las acciones pertinentes durante el ciclo de vida del mismo en las condiciones indicadas por el fabricante. De este modo, se asegura que los dispositivos de esta capa serán capaces de realizar su función de forma correcta en condiciones normales (excluyendo posibles problemas de funcionamiento o roturas propios de cualquier dispositivo). Con ello, se asegura la operatividad del sistema en elementos clave con gran impacto en el mismo, incluso en dispositivos que en muchas ocasiones deben tener un ciclo de vida a largo plazo, como sensores de paso de vehículos instalados en el propio asfalto.

Este tipo de sensores, que necesitan cumplir un nivel de exigencia alto, son costos, pero es necesaria la inversión para asegurar un sistema que cumpla su objetivo teniendo en cuenta la naturaleza y criticidad del mismo. Adicionalmente, también sería necesario realizar un análisis de eficiencia energética de los dispositivos antes de decantarse por una opción, ya que van a encontrarse en lugares donde la alimentación eléctrica no siempre está garantizada y deben poder utilizarse el mayor tiempo posible sin necesidad de sustituir el sistema de alimentación.

Lo ideal sería utilizar sistemas que aporten energía de forma continua, sin usar equipos de almacenamiento de energía (como baterías). Esto se podría conseguir utilizando alimentación de la red eléctrica, mediante alimentación vía red de datos (como Power over Ethernet o PoE[18]) o utilizando algún sistema de generación con almacenaje dedicado para uno o varios dispositivos

18 https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-power-over-ethernet.html

(paneles solares con baterías o aerogeneradores), ya que dadas las necesidades energéticas limitadas de los dispositivos, es posible utilizar equipos de pequeño tamaño para tal fin.

En la **capa de red**, se deben usar dispositivos que permitan la interconexión de los diferentes elementos teniendo en cuenta las necesidades de cada uno de ellos. Para la interconexión con la capa de sensorización, se deben utilizar dispositivos con especificaciones para uso en exterior en los casos en los que haya que ubicarlos cerca de los dispositivos, debido al uso al que van a estar sometidos y al emplazamiento en el que van a ser desplegados, además de ofrecer un buen nivel de señal para que la comunicación con el resto de equipos sea suficiente para ofrecer una calidad y potencia que permita al sistema operar de forma correcta. También se debería asegurar un sistema de comunicación secundario que pueda ser capaz de soportar la operación del sistema en caso de que el sistema primario falle, asegurando en la medida de lo posible la continuidad del servicio sin importar las eventualidades que puedan ocurrir.

Además, deben ofrecer medidas de seguridad lógica suficientes como para asegurar el acceso a los mismo únicamente por los elementos permitidos y el tráfico que transmiten. Otro punto clave es determinar qué tipo de tráfico viajará por cada uno de los dispositivos y elegir una tecnología acorde a dicho tráfico. Para los dispositivos de la capa de sensorización, probablemente la mejor opción sea una comunicación tipo máquina a máquina (M2M o “machine to machine”) propio de IoT para minimizar el uso de recursos y ancho de banda, de forma que se reduzca el consumo energético en dichos dispositivos.

Sin embargo, para la comunicación entre el resto de capas con uso de ancho de banda intensivo, los protocolos HTTP o TCP específicos serán lo más común. Por todo ello, lo más lógico es utilizar tecnologías de uso extendido y probado para las comunicaciones, como redes Wi-Fi o cableadas y la utilización de protocolos específicos IoT como MQTT y generalistas como HTTP para la comunicación entre los distintos elementos del sistema.

En la **capa de middleware** se utilizará un sistema en un proveedor cloud para ofrecer las capacidades necesarias para que los sensores y actuadores puedan conectarse al resto de elementos del sistema. En esta capa se establece el corazón del sistema de mensajería que recogerá toda la información que generan los sensores y la distribuirá a los elementos del sistema que deben procesarla para llevar a cabo acciones concretas, generar alertas o disparar flujos en otras partes del sistema. También se enviarán los cambios necesarios a los actuadores para que puedan llevar a cabo su cometido y modificar el entorno en caso de que sea necesario. Para ello, se debe establecer una configuración del sistema en alta disponibilidad, ya que el funcionamiento de dicho elemento es clave a la hora de mantener el sistema disponible y con operatividad suficiente para cumplir su cometido. La forma de lograr esto sería utilizar las capacidades del proveedor para armar un conjunto en el que el broker MQTT esté redundado con varias instancias que permitan la sincronización de datos entre ellas, de forma que cuando una de dichas instancias esté inoperativa, el resto puedan mantener la actividad y ofrecer el servicio al resto de elementos del sistema. De esta forma se logra ofrecer el servicio de mensajería como un elemento en alta disponibilidad como se comentó anteriormente, lo que aporta mayor estabilidad y resiliencia al mismo. Sin embargo, esto añade complicaciones al diseño, ya que se hace necesario añadir elementos como balanceadores de carga que pueden añadir dificultades a la hora de configurar y securizar el sistema. Si bien la configuración no afecta al objeto del presente trabajo, el aspecto de la seguridad sí puede añadir algún escollo importante si no se maneja de la forma adecuada.

En la **capa de gateway** también se va a utilizar un proveedor de servicios en la nube para diseñar la solución dadas las capacidades y soluciones que ofrece a la hora de manejar grandes volúmenes de datos desde multitud de orígenes diferentes. De este modo, se simplifica y centraliza el diseño de la solución, aportando integración nativa entre esta capa y la del middleware, estrechamente relacionadas. Adicionalmente, también ofrece capacidades avanzadas de autenticación y autorización de los elementos que se conectan al sistema, lo que aporta una capa de seguridad de gran valor a la hora de limitar accesos y permisos a los distintos componentes del sistema, además de permitir mantener un registro exhaustivo de las acciones y los accesos realizados por cada uno de los actores que operan en el sistema y detectar comportamientos anómalos o dañinos. Por último, permite el acceso a los sistemas en cloud desde infinidad de sistemas y utilizando conexiones seguras desde múltiples vías, como VPN, Ipsec, conexiones entre redes LAN en diferentes ubicaciones y un largo etcétera.

Para finalizar, también se utilizará las capacidades que ofrece el proveedor para diseñar la **capa de aplicación**, haciendo uso de los servicios que ofrece para aportar seguridad a dicha capa. Entre las características más valiosas que aporta un proveedor cloud a esta capa está el control de acceso y permisos unificado mencionado anteriormente, que permite establecer grupos de usuarios con accesos y permisos específicos, asegurando en todo momento qué acciones y sobre qué recursos tiene permiso una entidad dentro del sistema. Esta característica permite un alto grado de control sobre los activos de la capa de aplicación, limitando la superficie de ataque en caso de una intrusión en el sistema y la trazabilidad en caso de detectarse un ataque exitoso para determinar las acciones realizadas y los accesos logrados. También ofrece capacidades de tolerancia a fallos y alta disponibilidad para que la aplicación siga funcionando en caso de caída de alguno de los elementos que la conforman, lo que en un entorno sensible como el planteado es imprescindible. Por último, pero no menos importante, el proveedor aporta toda una colección de soluciones de seguridad entre las que destacan las soluciones de detección y prevención de intrusiones, mecanismos de protección frente a ataques de denegación de servicio, filtrado avanzado de tráfico y un largo etcétera.

A continuación se va a ofrecer un esquema conceptual del diseño del sistema, de modo que se pueda visualizar de forma sencilla cada una de las capas y qué parte ocupan dentro del sistema.

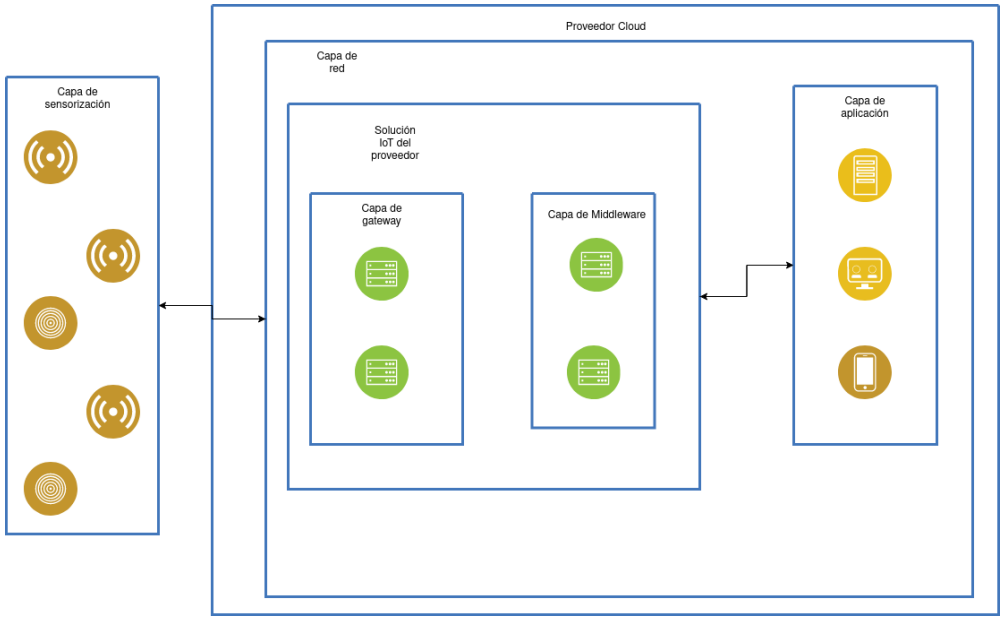

Figura 4: esquema de diseño del sistema IoT de control de tráfico planteado

Este caso se enmarcaría en el **Nivel Medio de requisitos de seguridad** de la metodología expuesta en el apartado 6, por lo que las medidas necesarias para el mismo se centrarán en conseguir un nivel de seguridad superior al del ejemplo anterior.

Con todo lo planteado hasta ahora, se van a analizar los requisitos de seguridad de cada una de las capas, profundizando en dichas necesidades y planteando soluciones a cada una de ellas de la forma más precisa y efectiva posible.

7.2.1 Capa de sensorización

La identificación y clasificación de los dispositivos que conforman la capa de sensorización resulta ser el primer paso fundamental. Esta tarea permitirá priorizar los activos en función de su relevancia para el correcto funcionamiento del sistema, proporcionando un enfoque basado en el valor y la criticidad de los mismos dentro del sistema. Con este enfoque, se puede establecer una línea base que define el comportamiento normal y el tráfico esperado generado por los dispositivos. Dicha línea base desempeñará un papel crucial en la detección temprana de posibles anomalías que podrían indicar la presencia de un ataque, aportando una defensa proactiva. En el sistema planteado, esto es posible de realizar utilizando las capacidades de Azure Monitor for IoT, una solución del proveedor de cloud que permite crear modelos de tráfico base del sistema y detectar cuando existen cambios significativos del mismo mediante soluciones de Machine Learning, detecciones que incluyen desde errores y caídas en el sistema hasta ataques.

La seguridad de los dispositivos en esta capa también requiere medidas que abarquen tanto el control de acceso por red al resto de elementos mediante cable como el acceso inalámbrico, sea cual sea la tecnología utilizada. En este sentido, la implementación de autenticación sólida y cifrado robusto en todas las comunicaciones entre los dispositivos y la infraestructura central se vuelve imperativa. Estos mecanismos garantizarán que solo los dispositivos validados puedan acceder al sistema y comunicarse de manera segura, reduciendo así el riesgo de acceso no autorizado. De este modo, se minimizan los **ataques de inyección de datos falsos, de interceptación e interferencia, ataques en arranque y ataques de drenaje de batería**, ya que la probabilidad de poder incluir elementos maliciosos en el sistema para interactuar con los dispositivos legítimos es prácticamente nula. Para realizar el despliegue y gestión de todo ello, los dispositivos de esta capa se conectarán a la solución del proveedor Azure IoT Hub, un servicio que ofrece características para cubrir todas las necesidades mencionadas. Por un lado, aporta un servicio de autenticación y autorización con control estricto de permisos utilizando un modelo de roles RBAC, y por otro lado permite controlar y gestionar que las conexiones que se realizan entre los dispositivos IoT y el broker de mensajería cumplan los requerimientos de seguridad definidos en el sistema. Además, permite utilizar las capacidades del proveedor para ofrecer soluciones tolerantes a fallos, en las que los puntos críticos del sistema se ofrecen en alta disponibilidad para minimizar el riesgo de caída del mismo.

En la dimensión física, la ubicación segura de los dispositivos y la restricción del acceso a ellos se convierten en medidas esenciales para prevenir **ataques físicos** que puedan comprometer la operatividad del sistema. Utilizar dispositivos de seguridad tradicionales como candados, alarmas o cámaras puede añadir una capa adicional de protección, previniendo potenciales

amenazas como robos o sabotajes. De esta forma, sería posible minimizar los **ataques de captura de nodo o inyección de código, así como los ataques en arranque** y la mayoría de **ataques de canal lateral** (ya que necesitar proximidad con el equipo para tener éxito). También es una medida efectiva el uso de sistemas diseñados para soportar daños físicos y ataques, como el apantallamiento de componentes electrónicos para evitar ataques de canal lateral.

Además, en este caso de estudio, se recomienda utilizar dispositivos que ofrezcan mecanismos de verificación de integridad proporcionados por los fabricantes. La verificación de la autenticidad y la integridad del hardware y del software o firmware de los dispositivos se convierte en un pilar de la seguridad. La utilización de firmware firmado y confiable, junto con herramientas de verificación y hardware dedicado en los dispositivos (TPM o similar), permitirá asegurar que los dispositivos no hayan sido objeto de modificaciones maliciosas o comprometidos de alguna manera.

7.2.2 Capa de red

En el análisis que ocupa el presente trabajo, es imprescindible abordar las necesidades de seguridad específicas en la capa de red. Esta capa, siendo un componente esencial para la comunicación fluida y segura, enfrenta una serie de amenazas que podrían comprometer la integridad y la disponibilidad de todo el sistema en cuestión. Dada la naturaleza crítica del caso de caso, es fundamental adoptar una estrategia de seguridad integral que aborde estas amenazas desde varios ángulos.

El primer paso en esta dirección implica contrarrestar el riesgo de **ataques de suplantación**, donde un atacante busca engañar al sistema haciéndose pasar por un dispositivo o entidad legítima. Para prevenir este tipo de ataques, es crucial implementar mecanismos sólidos de autenticación en la capa de red. Estos mecanismos asegurarán que solo los dispositivos y usuarios autorizados puedan acceder a la red, minimizando así la posibilidad de infiltración por parte de entidades no autorizadas. Es recomendable utilizar sistemas de validación de los equipos conectados a la red. Por ello, se recomienda el despliegue de sistemas de control de acceso a la red. Para entornos cableados, una posible solución sería utilizar FortiNAC[19], una solución que integra hardware y software para validar los dispositivos que se conectar a la red y establecer políticas y filtros para categorizarlos en función de reglas y patrones. En entornos Wi-Fi, es muy recomendable el uso de certificados para la asociación de los equipos a la red, de forma que únicamente los equipos legítimos puedan conectarse a la misma. Adicionalmente, añadir mecanismos de detección y prevención de intrusiones (IDS/IPS) es siempre una medida imprescindible en este tipo de sistemas.

El **acceso no autorizado** también es una amenaza latente en esta capa. Para mitigar este riesgo, se recomienda implementar medidas de control de acceso estrictas. Esto implica la configuración adecuada de políticas de acceso y la segmentación de la red en diferentes zonas con niveles de acceso definidos. La aplicación de firewalls y sistemas de detección de intrusiones puede proporcionar una barrera adicional de protección, identificando y bloqueando intentos de acceso no autorizado. Este tipo de medidas se deben implementar en todas las secciones que conforman la red, desde los sensores a los segmentos de red utilizados por las

19 https://www.fortinet.com/lat/products/network-access-control

máquinas y servicios desplegados en el proveedor. Al utilizar una solución propietaria, lo más operativo y sencillo de gestionar es el uso de los servicios de seguridad de red que se ofrecen en cloud, integrando los mismos en el servicio de seguridad Azure Security Center. De esta forma, es posible tener una visión general de todos los sistemas de seguridad desplegados en un mismo lugar.

Los **ataques de denegación de servicios (DoS)** representan una amenaza que podría afectar gravemente la disponibilidad del sistema. Como parte de las medidas de seguridad, es esencial implementar sistemas de mitigación de DoS que sean capaces de identificar patrones de tráfico malicioso y responder de manera efectiva para mantener la continuidad de la operación. Esto podría incluir la utilización de sistemas de balanceo de carga y la configuración de umbrales de tráfico anormal. La ventaja del uso de un proveedor cloud es la capacidad para tratar este tipo de ataques de forma innata, dadas las medidas de seguridad por defecto que nos ofrece y la capacidad de escalar los sistemas para soportar picos de tráfico en los elementos afectados, tales como endpoints de pasarelas de red y recursos de acceso VPN. Para los segmentos de red de sensores y actuadores, desplegar sistemas de filtrado de tráfico es también una opción más que recomendable, añadiendo límite de conexiones por dispositivo y filtrado de tráfico desde fuentes desconocidas o con un número de peticiones desproporcionado.

La **protección de los datos en tránsito** es otro aspecto crítico de la seguridad en la capa de red. Para abordar esta amenaza, se debe implementar cifrado robusto en todas las comunicaciones entre dispositivos y routers. Utilizar protocolos seguros como TLS (Transport Layer Security) garantizará que los datos transmitidos estén protegidos contra interceptación y manipulación. Dicho uso se debe establecer en la configuración de todos los elementos del sistema como pieza fundamental de la seguridad, añadiendo además controles de que se implementa en elementos de red como firewalls, IPS, redes privadas que conforman la parte de cloud del sistema IoT y cualquier otro elemento del sistema que ofrezca monitorización para verificar que todo el tráfico que se genera, procesa o gestiona dentro del sistema cuenta con las medidas de seguridad en tránsito oportunas. Además, con la ayuda de herramientas como Azure Monitor, Azure Network Watcher o Azure Security Center podemos verificar que se cumplen las necesidades requeridas.

Los **ataques de enrutamiento** también pueden tener un impacto significativo en la operación de la red. Dentro de esta agrupación, encontramos el ataque de sinkhole, que involucra la manipulación maliciosa del sistema de enrutamiento, donde un atacante desvía el tráfico hacia un nodo comprometido bajo su control. Para prevenir este tipo de ataque, se recomienda implementar sistemas de detección de enrutamiento anormal y mecanismos de autenticación de nodos. La monitorización constante de los patrones de tráfico y la detección de cambios repentinos en los flujos de datos pueden ayudar a identificar posibles desviaciones del enrutamiento esperado, permitiendo una respuesta temprana para contrarrestar este tipo de amenaza. Por otro lado, los ataques de worm-hole involucran la creación de un canal de comunicación directo y secreto entre dos nodos comprometidos en la red. Para hacer frente a este tipo de ataque, es vital implementar medidas de autenticación y cifrado robustas, utilizar protocolos de enrutamiento seguros y configuraciones que eviten la posibilidad de establecer rutas maliciosas. El uso de sistemas de detección de enrutamiento anómalo puede ser beneficioso para identificar posibles desviaciones del enrutamiento normal y tomar medidas correctivas. El despliegue de sistemas de monitorización de tráfico, junto con una supervisión de los sistema de enrutamiento y análisis de los logs proporciona una solución eficaz contra este tipo de ataques. Con herramientas como las mencionadas en la sección anterior, Azure Monitor

o Azure Network Watcher, es posible lograr una visión de los indicadores principales que pueden mostrar un ataque de este tipo y tomar las medidas oportunas.

7.2.3 Capa de middleware

La capa de middleware se enfrenta a amenazas que exigen estrategias de seguridad específicas para preservar la robustez y la continuidad del sistema, dado el cometido de la misma dentro del mismo. Al ejercer funciones de intermediaria entre el resto de capas, lo que le permite obtener acceso a ellas y a los elementos que las conforman, además de aglutinar y procesar gran parte de los datos que se manejan en el sistema, es un punto de interés clave para los atacantes.

Los **ataques de signature wrapping**, que se centran en la manipulación de firmas XML en servicios web de middleware, son una amenaza sutil pero potencialmente devastadora. Para fortalecer la seguridad en esta área, es crucial implementar protocolos de firmado y validación de mensajes. La adopción de algoritmos de firma seguros y la utilización de técnicas de protección de mensajes XML, como la firma ciega o la verificación de firmas cruzadas, pueden dificultar los intentos de los atacantes de explotar vulnerabilidades en el protocolo SOAP. Utilizar certificados para validar la identidad de los orígenes es también una de las medidas más efectivas contra este tipo de ataques, además de ejercer un estricto control de identidad en cuanto a la autenticación y autorización de todas las entidades del sistema, para lo que el proveedor nos ofrece la herramienta ya mencionada (Azure AD).

El riesgo de un **ataque de inyección SQL** tampoco puede pasarse por alto en la capa de middleware. Las posibles vulnerabilidades en las consultas SQL pueden llevar a la exposición de datos confidenciales o incluso al compromiso de la integridad de las bases de datos. Para abordar esta amenaza, es imperativo implementar medidas sólidas de validación y filtrado de entradas. La adopción de consultas parametrizadas y el uso de bibliotecas de acceso a bases de datos que proporcionan protección contra inyecciones SQL son esenciales. Además, establecer un control de acceso riguroso basado en roles y minimizar los privilegios de acceso ayudará a reducir la superficie de ataque y prevenir posibles explotaciones de inyecciones SQL. Este tipo de ataques a las bases de datos del middleware pueden mitigarse utilizando tanto mecanismos de seguridad de la capa de red como firewalls como soluciones propias. En este caso, Azure SQL Database ofrece reglas de firewall de bajo nivel para limitar el número de orígenes con acceso a la base de datos, lo que limita los elementos que pueden interactuar con la misma.

Los **ataques Man in the Middle (MitM)** plantean una preocupación constante en la capa de middleware. Para fortalecer la seguridad en esta área, es crucial implementar medidas de autenticación y cifrado sólidos. La adopción de protocolos criptográficos confiables, como TLS, garantizará la confidencialidad e integridad de las comunicaciones entre los componentes del sistema. Además, la autenticación de dos factores y el uso de certificados digitales reforzarán la legitimidad de los dispositivos que operan en el sistema y dificultarán los intentos de atacantes de interceptar y manipular la comunicación entre los componentes. Para todo ello, existen multitud de soluciones integradas, como las que se han ido comentando a lo largo del trabajo, para establecer controles y monitorizar el cumplimiento de los mismos, como Azure Monitor, Azure Security Center y Azure Sentinel entre los más destacados.

7.2.4 Capa de gateway

La capa de pasarela (gateway) es susceptible a diversas amenazas que requieren un enfoque proactivo en materia de seguridad para asegurar la funcionalidad, la integridad y la confidencialidad del sistema, dada la importancia de la misma dentro del sistema al gestionar los datos que se transfieren por el sistema, así como los puntos de interconexión entre las distintas redes y los sistemas que controlan dichas interconexiones y accesos a diferentes capas del sistema.

Los **ataques a las actualizaciones de firmware** presentan un riesgo significativo, ya que un atacante podría explotar esta debilidad del sistema para inyectar código malicioso y comprometer los equipos que utilizan el gateway para actualizar su firmware o software. Para contrarrestar esta amenaza, es esencial implementar una estrategia de gestión de actualizaciones rigurosa. Esto implica la verificación y validación exhaustiva de las actualizaciones antes de su implementación, así como la utilización de firmas digitales para garantizar la autenticidad e integridad de las actualizaciones. Además, se recomienda establecer un proceso de recuperación segura en caso de que una actualización maliciosa se haya aplicado. En este caso, el proveedor elegido para el caso de estudio aporta una solución específica para esta casuística, que permite desplegar actualizaciones desde la propia infraestructura en la nube, aportando seguridad y verificando cada una de las partes para que no sea necesario hacerlo de forma manual o implementando un costoso sistema paralelo.

Los **ataques al cifrado de extremo a extremo** en la capa de pasarela plantean un riesgo a la confidencialidad y la integridad de los datos transmitidos entre los dispositivos conectados y la capa de aplicación. Para abordar esta amenaza, es fundamental implementar un cifrado robusto en las comunicaciones. La utilización de protocolos criptográficos seguros, como TLS (Transport Layer Security), garantizará que los datos en tránsito estén protegidos contra cualquier intento de interceptación. La gestión adecuada de claves y certificados digitales también es esencial para mantener la confiabilidad del sistema de cifrado. Además, la monitorización constante del estado del cifrado permitirá identificar y responder de manera proactiva a cualquier anomalía en la seguridad de las comunicaciones. Todo ello es posible con las soluciones de conexión entre diferentes entornos que proporciona Azure, tanto a nivel interno dentro de su propia infraestructura como de interconexión con el resto de componentes del sistema (en este caso los dispositivos IoT con su red independiente). Los servicios de Azure Security Center, Azure Monitor y Azure Network Watcher ofrecen capacidades para controlar que el tráfico navega cifrado dentro del sistema. Azure VPN Gateway y Azure ExpressRoute permiten conectar distintos entornos de red independientes con la infraestructura del proveedor al nivel necesario, de forma que todos los dispositivos tengan la conectividad requerida entre ellos bajo un estricto control de seguridad y de la forma más simple y eficaz posible.

Los **ataques a interfaces innecesarias** en la capa de pasarela aprovechan la exposición de puntos de entrada no deseados, que pueden ser utilizados por los atacantes para obtener acceso no legítimo al sistema. Para mitigar este riesgo, es fundamental seguir el principio de mínimo privilegio y deshabilitar todas las interfaces que no sean esenciales para el funcionamiento de la pasarela mediante la configuración. La implementación de firewalls y mecanismos de control de acceso (ACLs) permitirá filtrar y bloquear cualquier tráfico no autorizado. Además, la segmentación de red también puede ser una medida efectiva para aislar la pasarela y limitar la exposición de interfaces no esenciales a posibles atacantes. En cuanto a posibles medidas

adicionales, Azure ofrece sus soluciones de Firewall para filtrar el tráfico cuyo destino sea cualquier interfaz de red diferente a la utilizada para el normal funcionamiento del sistema.

El **secure on-boarding de dispositivos** en el sistema es también crucial para prevenir la incorporación de dispositivos no autorizados en la capa de pasarela. La autenticación y autorización sólidas de dispositivos durante el proceso de on-boarding son esenciales para garantizar que solo los dispositivos legítimos sean admitidos en la red. Para lograrlo, se debe implementar un proceso de registro seguro que involucre el intercambio de claves y certificados digitales. La utilización de mecanismos como la autenticación cruzada mediante certificados y el análisis de comportamiento de dispositivos durante el proceso de on-boarding también aumentará la seguridad en esta fase crítica. Para ello, el proveedor elegido en este caso ofrece una solución automática que ofrece todas las medidas comentadas para realizar la inclusión segura en el sistema de los dispositivos. Dicho servicio se llama Azure IoT Hub Device Provisioning Service, y ofrece un conjunto de operaciones para configurar el dispositivo con los parámetros necesarios de forma dinámica y cumpliendo los requisitos de seguridad, lo que aporta flexibilidad al sistema.

7.2.5 Capa de aplicación

La capa de aplicación se encuentra expuesta a diversas amenazas que requieren un análisis profundo para garantizar la seguridad integral del sistema. Esto es debido a que en dicha capa es donde se manipulan los datos y se toman las decisiones tanto operativas como a nivel de dirección y gestión estratégica del mismo. También es un punto significativo para los atacantes dado que se podría controlar la práctica totalidad del mismo y extraer la información más significativa, lo que implica un interés primordial. Por ello, se va a analizar cada una de las amenazas asociadas a la misma, así como posibles medidas a implantar en el contexto del caso concreto.

El **ataque de robo de datos** plantea una preocupación significativa ya que, podría resultar en la filtración de información crítica, como datos de tráfico en tiempo real, patrones de movilidad de los ciudadanos y planificación de rutas. Para abordar esta amenaza, es esencial implementar técnicas de encriptación de datos tanto en reposo como en tránsito. El uso de algoritmos criptográficos sólidos garantizará la confidencialidad de los datos, mientras que la gestión adecuada de claves y la rotación regular de las mismas reducirán el riesgo de exposición en caso de compromiso. Además, es necesario aplicar mecanismos de enmascaramiento de los datos siempre que sea posible, dado que en caso de que un ataque sea exitoso, la obtención de la información original y los datos privados recogidos sin el algoritmo de desenmascarado será mucho más costoso de recuperar para los atacantes, haciendo su uso posterior prácticamente inviable. Estas características nos las ofrece Azure para sus soluciones de base de datos, tanto a nivel de cifrado como de enmascaramiento de los datos en uso, por lo que los datos siempre estarían seguros en la medida que se defina el uso de dichas capacidades.

El **ataque sobre el control de accesos** representa un riesgo considerable en la capa de aplicación, ya que un acceso no autorizado podría permitir a los atacantes manipular la configuración de semáforos, desviar el tráfico o causar bloqueos en puntos críticos. Para mitigar esta amenaza, es esencial implementar un modelo de autenticación y autorización sólido. La

implementación del principio de menor privilegio asegurará que los usuarios solo tengan acceso a las funciones y datos necesarios para sus roles específicos. La autenticación multifactor y la monitorización constante de los registros de actividad permitirán detectar y responder a intentos de acceso no autorizado. Azure mantiene todo su sistema de roles y permisos en la solución centralizada Azure AD, lo que permite controlar a un nivel muy bajo los usuarios y grupos existentes y el nivel de permisos para cada uno de ellos, todo ello en un elemento centralizado y mantenido por el proveedor. Además, ofrece multitud de mecanismos para autenticar a los elementos del sistema, tanto usuarios como dispositivos o elementos del sistema, de forma que la suplantación es muy compleja de llevar a cabo con sistemas como la autenticación con dos factores. Todo ello aporta una característica adicional, y es que permite tener un control exhaustivo y pormenorizado de las acciones que se realizan en el sistema y quién las ha realizado.

El **ataque de interrupción del servicio** plantea un riesgo a la disponibilidad y la continuidad de la operación en la capa de aplicación. Si los atacantes logran interrumpir los servicios, los usuarios legítimos no podrán utilizarlo, lo que causaría en la práctica una caída del mismo. En este caso, los atacantes tratan de interrumpir el servicio agotando los recursos de las aplicaciones del sistema, lo que impediría manejar el sistema y realizar acciones sobre el mismo durante el tiempo que dure dicho ataque. Para evitarlo, las capacidad de escalabilidad y tolerancia a fallos de los entornos cloud se presentan como los mayores aliados. En este caso, un diseño con redundancia geográfica y replicación de los recursos dentro de cada geografía proporcionan una solución más que eficaz contra este tipo de ataques. Además, la infraestructura de Azure aporta protección adicional con la solución Azure DDoS Protection.

El **ataque de inyección de código** representa una seria amenaza para la integridad y el funcionamiento de la capa de aplicación. Los atacantes podrían insertar código malicioso que altere la lógica de funcionamiento de la aplicación y afecte su comportamiento normal. Para abordar este riesgo, es esencial implementar prácticas sólidas de desarrollo seguro de software. La validación y filtrado adecuado de las entradas de usuario ayudarán a prevenir inyecciones de código, mientras que la implementación de firewalls a nivel de aplicación, con capacidad para diseccionar y analizar el tráfico que llega al aplicativo, detectará y bloqueará intentos maliciosos. Azure ofrece una amplia gama de soluciones que pueden ayudar a reducir este tipo de ataques, como un WAF (web application firewall) con reglas específicas para inyecciones de todo tipo. Además se integra en la consola de eventos y orquestación de seguridad Azure Sentinel para la gestión unificada de los eventos de seguridad.

El **ataque de interceptación de datos** pone en peligro la confidencialidad de la información transmitida entre la capa de aplicación y los dispositivos conectados. Para mitigar este riesgo, es esencial implementar el cifrado en todas las comunicaciones. El uso de protocolos criptográficos sólidos como TLS garantizará que los datos en tránsito estén protegidos contra cualquier intento de interceptación. Además, la implementación de mecanismos de detección de intrusos y la supervisión constante de las comunicaciones permitirán identificar actividades sospechosas y responder de manera proactiva. Es posible lograr todo ello, como se ha comentado, haciendo uso de las herramientas de seguridad de Azure, como Azure Sentinel, que permite monitorizar y analizar eventos de seguridad de forma centralizada al tiempo que tomar acciones o validar la eficacia de las medidas automáticas aplicadas en cada caso.

8 Conocimiento extraído y conclusiones

A lo largo de este trabajo, se ha podido comprender la problemática de la seguridad en los sistemas IoT, teniendo en cuenta las particularidades de los mismos, las diferentes tecnologías que integran y la dificultar para encontrar guías en las que se analicen amenazas específicas para este tipo de sistemas.

Al inicio, se han sentado las bases de las necesidades de este tipo de sistemas en cuanto a requisitos de seguridad, la dificultad para identificarlas y los conceptos básicos sobre el ámbito de la seguridad y los sistemas IoT para abordar los siguientes apartados.

Una vez hecho esto, se ha presentado una clasificación de las amenazas que pueden sufrir este tipo de sistemas, basadas en referencias a frameworks y normativas de relevancia dentro del ámbito de la ciberseguridad. Además, se ha planteado una batería de posibles medidas correctivas para cada una de ellas, de forma que se ofrece una base de conocimiento para que el lector sea capaz de analizar diferentes amenazas, comprender cómo y porqué pueden suponer un riesgo para el sistema y qué solución conceptual debería aplicarse para minimizar el riesgo de la misma.

Con todo ello, se ha propuesto una metodología para ayudar a categorizar riesgos y plantear soluciones para los mismos, de forma que se pueda utilizar dicha metodología en el análisis de cualquier sistema IoT que cumpla los requisitos especificados al inicio del trabajo.

Para comprobar la metodología propuesta y ofrecer ejemplos de aplicación de la misma, se han presentado dos casos de estudio. En dichos casos, se ha podido aplicar todo lo expuesto sobre dos ejemplos de sistemas ficticios, pero con suficiente nivel de detalle en su diseño como para clarificar todo lo analizado en el trabajo.

En dichos casos, se han podido extraer varias conclusiones sobre las amenazas más comunes y que más impacto pueden tener sobre los sistemas IoT. A continuación se exponen las más relevantes:

- Los sistemas IoT se enfrentan a un gran número de amenazas diferentes. Algunas de ellas son conocidas por estar directamente relacionadas con la seguridad IT tradicional, pero otras son específicas y necesitan de un análisis específico.
- La protección de la confidencialidad y la integridad de la información en tránsito es crucial y las medidas necesarias para asegurarla son relativamente sencillas y baratas de implementar.
- La segmentación de la red se presenta como una táctica imprescindible para minimizar la exposición a amenazas en todas las capas.
- La aplicación de medidas enfocadas a minimizar o eliminar las principales amenazas proporciona seguridad a más de una capa al mismo tiempo, por lo que la aplicación de las mismas produce un aumento significativo del nivel de seguridad general del sistema (utilización de cifrado, segmentación de red, monitorización, etc.).

- La aplicación de medidas para las amenazas menos probables, como los ataques de canal lateral (apartado 4.1) son costosa y únicamente tiene sentido su implantación en sistemas que se enmarquen en el Nivel Alto de requisitos de seguridad planteados en el apartado 6.

Con todo lo anterior, el lector dispone de una directrices suficientes para acometer el análisis de diseños de sistemas IoT de infinidad de tipos (excluyendo los sistemas que quedan fuera del ámbito del trabajo).

9 Referencias

1. C. -L. Zhong, Z. Zhu and R. -G. Huang. (2015). Study on the IOT Architecture and Gateway Technology. Study on the IOT Architecture and Gateway Technology | IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/7429590

2. Computer Security Incident Handling Guide. (n.d.). NIST Technical Series Publications. Retrieved Julio 18, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

3. Current research on Internet of Things (IoT) security: A survey | Request PDF. (2018, December). ResearchGate. Retrieved Marzo 22, 2023, from https://www.researchgate.net/publication/329351471_Current_research_on_Internet_of_Things_IoT_security_A_survey

4. CWE - CWE-20: Improper Input Validation (4.12). (n.d.). Common Weakness Enumeration. Retrieved Junio 21, 2023, from https://cwe.mitre.org/data/definitions/20.html

5. CWE - CWE-347: Improper Verification of Cryptographic Signature (4.12). (n.d.). Common Weakness Enumeration. Retrieved Julio 22, 2023, from https://cwe.mitre.org/data/definitions/347.html

6. CWE - CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') (4.12). (n.d.). Common Weakness Enumeration. Retrieved Julio 25, 2023, from https://cwe.mitre.org/data/definitions/74.html

7. CWE - CWE-94: Improper Control of Generation of Code ('Code Injection') (4.12). (n.d.). Common Weakness Enumeration. Retrieved Julio 28, 2023, from https://cwe.mitre.org/data/definitions/94.html

8. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (2018, April 16). NIST Technical Series Publications. Retrieved Julio 14, 2023, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

9. Glosario. (n.d.). CCN-CERT. Retrieved Enero 22, 2023, from https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html

10. G. Restuccia, H. Tschofenig and E. Baccelli. (2020). Low-Power IoT Communication Security: On the Performance of DTLS and TLS 1.3. Retrieved Julio 22, 2023, from https://ieeexplore.ieee.org/abstract/document/9293085

11. Guidelines for securing Wireless Local Area Networks (WLANs). (n.d.). NIST Technical Series Publications. Retrieved Julio 15, 2023, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf

12. Guide to Industrial Control Systems (ICS) Security. (n.d.). NIST Technical Series Publications. Retrieved Julio 14, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

13. IEC 27001 Standard – Information Security Management Systems. (n.d.). ISO. Retrieved September 8, 2023, from https://www.iso.org/standard/27001

14. IoTSF Secure Design Best Practice Guide. (n.d.). IoT Security Foundation. Retrieved Julio 25, 2023, from https://www.iotsecurityfoundation.org/wp-content/uploads/2019/03/Best-Practice-Guides-Release-1.2.1.pdf

15. Koen Zandberg; Kaspar Schleiser; Francisco Acosta; Hannes Tschofenig; Emmanuel Baccelli. (2020). Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check. Retrieved Julio 19, 2023, from https://ieeexplore.ieee.org/abstract/document/8725488

16. Microsoft. (n.d.). Azure IoT: plataforma de Internet de las cosas. Microsoft Azure. Retrieved Mayo 18, 2023, from https://azure.microsoft.com/es-es/solutions/iot/

17. MITRE. (n.d.). Common Vulnerabilities and Exposures. CVE - CVE. Retrieved Junio 15, 2023, from https://cve.mitre.org/

18. NIST Security and Privacy Controls for Information Systems and Organizations. (2020, September 5). NIST Technical Series Publications. Retrieved Julio 24, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

19. NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11l. (2007, Febrero). NIST Technical Series Publications. Retrieved Julio 30, 2023, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf

20. NIST Special Publication 800-63B. (2017, June). NIST Pages. Retrieved Julio 26, 2023, from https://pages.nist.gov/800-63-3/sp800-63b.html

21. NIST Special Publication (SP) 800-189, Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation. (2019, December 17). NIST Computer Security Resource Center. Retrieved Mayo 22, 2023, from https://csrc.nist.gov/pubs/sp/800/189/final

22. NIST Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management. (n.d.). Retrieved Julio 25, 2023, from https://www.nccoe.nist.gov/sites/default/files/2022-12/iot-onboarding-nist-sp1800-36a-preliminary-draft.pdf

23. Open Worldwide Application Security Project (OWASP). (2021). OWASP Top 10:2021. Retrieved Mayo 12, 2023, from https://owasp.org/Top10/

24. OWASP IoT Project 2014-I2. (n.d.). Retrieved Julio 25, 2023, from https://wiki.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization

25. OWASP Mobile Application Security. (n.d.). OWASP Foundation. Retrieved Julio 28, 2023, from https://owasp.org/www-project-mobile-app-security/

26. OWASP Web Security Testing Guide. (n.d.). OWASP Foundation. Retrieved Julio 29, 2023, from https://owasp.org/www-project-web-security-testing-guide/

27. Paul Fremantle, Philip Scott. (2017, May 8). *A survey of secure middleware for the Internet of Things*. PeerJ. Retrieved Febrero 12, 2023, from https://peerj.com/articles/cs-114/

28. Recommendation for Key Management: Part 1 - General. (2020, May 5). NIST Technical Series Publications. Retrieved Julio 11, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

29. R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan. (2015). *Internet of things (IoT) security: Current status, challenges and prospective measures*. Retrieved Enero 24, 2023, from https://ieeexplore.ieee.org/abstract/document/7412116

30. SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (2011, September). NIST Technical Series Publications. Retrieved Agosto 04, 2023, from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf

31. SP 800-183, Networks of 'Things' | CSRC. (2016, July 28). NIST Computer Security Resource Center. Retrieved September 8, 2023, from https://csrc.nist.gov/pubs/sp/800/183/final

10 Anexo - ODS

OBJETIVOS DE DESARROLLO SOSTENIBLE

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No Procede
ODS 1. **Fin de la pobreza.**		X		
ODS 2. **Hambre cero.**			X	
ODS 3. **Salud y bienestar.**	X			
ODS 4. **Educación de calidad.**			X	
ODS 5. **Igualdad de género.**			X	
ODS 6. **Agua limpia y saneamiento.**		X		
ODS 7. **Energía asequible y no contaminante.**		X		
ODS 8. **Trabajo decente y crecimiento económico.**		X		
ODS 9. **Industria, innovación e infraestructuras.**	X			
ODS 10. **Reducción de las desigualdades**.			X	
ODS 11. **Ciudades y comunidades sostenibles**.	X			
ODS 12. **Producción y consumo responsables.**		X		
ODS 13. **Acción por el clima.**	X			
ODS 14. **Vida submarina.**			X	
ODS 15. **Vida de ecosistemas terrestres.**		X		
ODS 16. **Paz, justicia e instituciones sólidas.**	X			
ODS 17. **Alianzas para lograr objetivos.**		X		

En la era de la digitalización, la interconexión de dispositivos a través del Internet de las Cosas (IoT) se ha convertido en un motor fundamental para la transformación tecnológica y el avance hacia un futuro más eficiente y conectado.

Sin embargo, con la promesa de innovaciones revolucionarias también surge la necesidad de salvaguardar la seguridad y la integridad de estos sistemas.

El análisis de las amenazas a la seguridad en sistemas IoT no solo constituye una necesidad esencial de la ciberseguridad en el mundo actual, sino que también presenta una influencia significativa en el logro de los Objetivos de Desarrollo Sostenible (ODS) establecidos por la Agenda 2030 de las Naciones Unidas. Esta relación intrínseca entre la seguridad en sistemas IoT y los ODS se traduce en un potencial transformador para un futuro más sostenible y equitativo para todos.

El desarrollo expuesto en este trabajo guarda relación con la mayoría de los aspectos tratados por los Objetivos de Desarrollo Sostenibles, siendo los siguientes los que guardan más relación en la medida descrita en cada apartado.

ODS 3: Salud y Bienestar

La seguridad en los sistemas IoT es crucial en el ámbito de la salud, donde la integridad y confidencialidad de los datos son de suma importancia. Desde dispositivos médicos conectados hasta la gestión de datos de pacientes, garantizar la seguridad en estos sistemas contribuye a la mejora de la atención sanitaria y el bienestar de la población.

ODS 9: Industria, Innovación e Infraestructura

El despliegue masivo de dispositivos IoT impulsa la innovación en diversos sectores, desde la salud hasta la agricultura y la gestión urbana. Sin embargo, este crecimiento también trae consigo un aumento en la superficie de ataque. Es esencial invertir en infraestructuras seguras y fomentar la innovación responsable para garantizar que los sistemas IoT contribuyan positivamente al desarrollo sostenible.

ODS 11: Ciudades y Comunidades Sostenibles

Los sistemas IoT tienen el potencial de transformar nuestras ciudades en espacios más eficientes y habitables. Desde la gestión de residuos hasta la optimización del transporte público, la implementación segura de este tipo de dispositivos puede contribuir a ciudades más sostenibles y resilientes.

ODS 13: Acción por el Clima

La gestión eficiente de la energía es un pilar fundamental en la seguridad de los sistemas IoT. La adopción de prácticas que reduzcan el consumo energético y promuevan el uso de fuentes renovables, gracias al despliegue de este tipo de sistemas, puede influir en gran medida para mitigar el impacto ambiental y contribuir a la lucha contra el cambio climático.

ODS 16: Paz, Justicia e Instituciones Sólidas

La seguridad en los sistemas IoT tiene implicaciones directas en la protección de la privacidad y los derechos de los individuos. Establecer marcos legales y regulaciones sólidas es esencial para garantizar que la implementación de dispositivos IoT respete los derechos humanos y promueva un entorno seguro y confiable.

En conclusión, abordar las amenazas y riesgos de seguridad en sistemas IoT no solo es una necesidad tecnológica, sino que también está intrínsecamente ligada a los Objetivos de Desarrollo Sostenible de la Agenda 2030. Al tratar de garantizar una implantación segura y responsable de este tipo de sistemas, contribuimos al avance hacia un futuro más sostenible, inclusivo y equitativo para todos.