Universitat Oberta de Catalunya

uoc.edu

Seguridad en la Internet de las cosas

Irene Salas Sanz
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Ciberseguridad

Ángela María García
Víctor García Font

04 junio 2019

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Seguridad en la Internet de las cosas*
Nombre del autor:	*Irene Salas Sanz*
Nombre del consultor/a:	*Ángela María García*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2019
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área del Trabajo Final:	*Ciberseguridad*
Idioma del trabajo:	*Castellano*
Palabras clave	*IoT, OWASP, riesgo*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

El trabajo de final de máster consiste en la realización de un estudio sore la ciberseguridad en el Internet of Things (IoT), analizando sus amenazas, riesgos y vulnerabilidades. Para ello se describe cómo se establece la interconexión digital de objetos cotidianos con Internet, identificando los riesgos que presenta, las amenazas a las que se enfrenta y las mejores prácticas a llevar a cabo para proteger y analizar las vulnerabilidades asociadas. La OWASP (Open Web Application Security Project) identifica los diez riesgos más comunes y críticos basándose en la OWASP Risk Rating Methodology para priorizar. Para llevar a cabo este trabajo nos basaremos en la metodología OWASP para identificar los riesgos a los que se enfrenta IoT.

Abstract (in English, 250 words or less):

The final work of the master consists in a study on cybersecurity in the Internet of Things (IoT), analyzing its threats, risks and vulnerabilities. For this, it is described how the digital interconnection of everyday objects with the Internet is established, identifying the risk it presents, the threats it faces and the best practices to be carried out to protect and analyze the associated vulnerabilities. The OWASP (Open Web Application Security Project) identifies the ten most common and critical risks based on the OWASP Risk Rating Methodology to prioritize. To carry out this work, we will use the OWASP methodology to identify the risks that IoT faces.

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1 Contexto y justificación del Trabajo

Desde hace unos años se empezó a hablar del IoT (Internet de las cosas), como una apuesta de futuro y hoy por hoy ha comenzado a ser una realidad. El Internet de las cosas se ha convertido en un elemento más en nuestras vidas cotidianas. Gracias al IoT hay una mayor integración entre el mundo real y el tecnológico para dar solución a infinitos problemas. Cada vez es más frecuente encontrarse con nuevos dispositivos capaces de conectarse a Internet y permitir al usuario un control y manejo de forma remota desde cualquier parte del mundo. Sin embargo, la rápida y constante evolución de estas tecnologías, deja su seguridad rezagada, lo que supone un foco importante de riesgos, amenazas y vulnerabilidades, aunque también de desarrollo de nuevas oportunidades y soluciones.

Los riesgos asociados a la seguridad y privacidad que se derivan de este nuevo ecosistema interconectado es uno de los principales retos a los que hace frente el IoT. Cada vez tenemos más aparatos conectados en casas y empresas, que nos facilitan la vida y nos permiten controlarlo todo estemos donde estemos, pero se puede intuir la gran cantidad de problemas de ciberseguridad y privacidad de la información que pueden afectar a los usuarios. Todo lo que está conectado a Internet es vulnerable a ser hackeado, por lo que todos los objetos o dispositivos IoT están expuesto a sufrir ataques cibernéticos. Cuando usamos nuestros dispositivos móviles (Smartphones) u ordenadores, dejamos un rastro de actividad, una serie de registros que nos hacen estar expuestos a diferentes riesgos como: usurpación o suplantación de identidad, escuchas secretas (sniffer), denegación de servicios (DDos), robo de contraseñas, malware, etc. [1]

El IoT es una red de redes donde una gran cantidad de objetos o dispositivos se alojan y se pueden conectar entre sí. Es decir, se podrían interconectar a esa red todos los objetos que se pueda imaginar como vehículos, electrodomésticos, dispositivos mecánicos, u objetos tales como muebles, calzado, maletas, dispositivos de medición, etc. El objetivo que se pretende alcanzar con dicha tecnología, así como con la gran mayoría de avances tecnológicos, es hacer más cómodas nuestras vidas así como proporcionar una mayor seguridad en diversos ámbitos. Un frigorífico podría ser capaz de advertirnos si un alimento está caducado o pasado, o podríamos tener el control de nuestra casa desde nuestros dispositivos móviles. Podríamos saber en cualquier momento la ubicación exacta de dichos dispositivos, evitando su extravío, así como saber cómo se consumen en el mundo o si están encendidos o apagados en todo momento.

Pero ¿cómo se establece la conexión en IoT? Por un lado se establece la conexión a través de una IP de los objetos, es decir, los objetos con los que las personas o usuarios nos relacionamos vía Internet tienen una IP asignada que envía información (datos que proporcionamos al usarlos) a un servidor. La forma en la que los usuarios recogemos esa información es a través de una WI-FI, un Bluetooth, un RFID o código QR, etc. Por otro lado se establece la

conexión M2M (Machine to Machine), que es la comunicación entre los diversos objetos conectados a Internet, sin la intervención de los usuarios. [1]

Este concepto de IoT nació en el Instituto de Tecnología de Massachusetts (MIT) entre el año 2008 y el 2009 y en un principio hacía referencia a la conexión a Internet de sensores, vehículos, máquinas y todo tipo de objetos. Con estas conexiones se buscaba mejorar las labores de mantenimiento y seguridad en ciudades, viviendas, comercios, transporte, etc. Se calcula que en el año 2020 entre 22.000 y 50.000 millones de dispositivos se conectarán a Internet para ofrecer a los ciudadanos servicios y aplicaciones inteligentes. Según los datos facilitados por Gartner, en el año 2020 se calcula que el número de objetos conectados será de 26.000 millones mientras que en 2009 había cerca de 900 millones, es decir unas treinta veces más

1.2 Objetivos del Trabajo

Para la realización de este trabajo de final de máster se definen los siguientes objetivos a llevar a cabo:

- Realizar un estudio sobre los diferentes riesgos y amenazas asociados a IoT.

- Realizar una guía sobre las mejores prácticas para estar protegido de los riesgos y amenazas relacionados con IoT.

- Realizar un estudio en profundidad sobre las vulnerabilidades asociadas.

1.3 Enfoque y método seguido

La metodología OWASP de IoT [3] está diseñada para ayudar a entender los riesgos de internet asociados con IoT, permitiendo a los usuarios tomar las mejores decisiones de seguridad a la hora de diseñar, construir y desarrollar la tecnología IoT. Ésta define el Top 10 2018 de los riesgos asociados a IoT:

1. Uso de contraseñas débiles o en texto plano.
2. Uso de servicios de red inseguros.
3. Uso de interfaces inseguras.
4. La falta de un mecanismo seguro de actualización de firmware.
5. Uso de librerías inseguras o desactualizadas.
6. Insuficiente protección de la información personal o privada.
7. Almacenamiento y transferencia de datos insegura.
8. La falta de gestión remota de dispositivos.
9. Uso de parámetros por defecto inseguros.
10. Falta de seguridad física en los dispositivos.

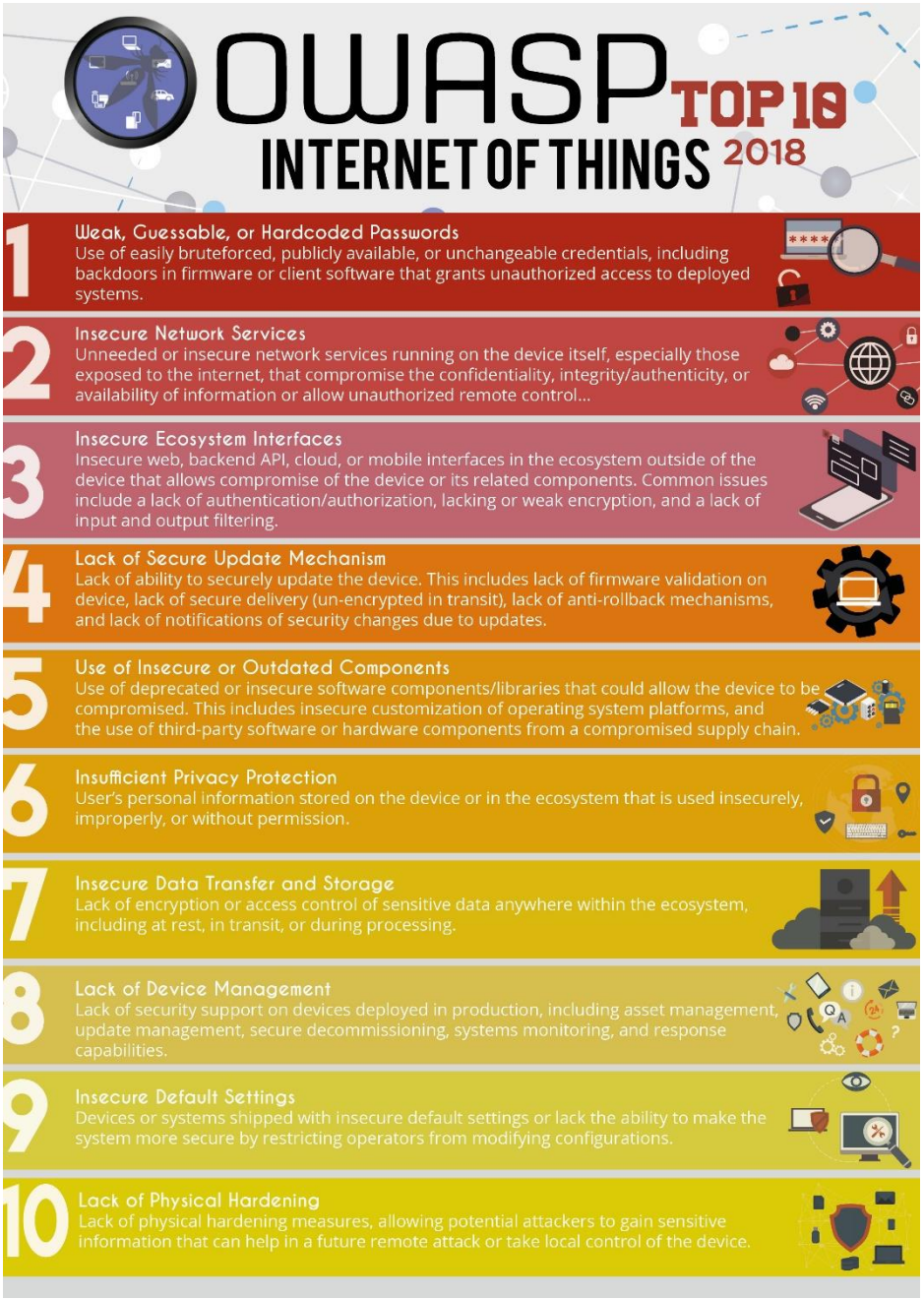

Figure 1: Top 10 OWASP IoT

1.3.1 Metodología OWASP Risk Rating Management [2]

La metodología de medición del riesgo de OWASP es un sistema establecido de medición de riesgos que estima la severidad de éstos hacia la empresa u organización, ayudando a ahorrar tiempo y priorizando los riesgos más serios, para garantizar la correcta toma de decisión a la hora de establecer las medidas para mitigarlos.

Para valorar el riesgo se debe de tener en cuenta que una vulnerabilidad crítica para un tipo de empresa no lo es para otra y por tanto las consecuencias que ésta tiene en la organización pueden variar de la misma manera. La

OWASP establece la severidad del riesgo mediante una metodología estándar, personalizado para la seguridad en las aplicaciones, mediante el siguiente modelo estándar:

Riesgo = Probabilidad x Impacto

Los factores implicados en la “Probabilidad” e “Impacto” para la seguridad de aplicaciones y que constituyen esta metodología son los siguientes:

- Identificar el riesgo:

Para identificar un riesgo de seguridad que necesita ser tratado es necesario identificar los agentes de amenaza, las vulnerabilidades que pueden ser explotadas por las amenazas y estimar el impacto sobre el negocio en el caso de que una amenaza se materialice.

- Estimar la probabilidad:

Una vez identificados los riesgos, es necesario estimar la probabilidad de que una vulnerabilidad en particular sea descubierta y explotada, y cuantificarla:

ALTO/ HIGH	Vulnerabilidad que si es explotada comprometería la seguridad de la información ocasionando un impacto negativo sobre la empresa. Debe solucionarse inmediatamente
MEDIO/MEDIUM	Vulnerabilidad que si es explotada tendría un impacto leve sobre la operativa del negocio. Puede solucionarse en un tiempo prudente.
BAJO/ LOW	Vulnerabilidad que si es explotada no ocasionaría mayores inconvenientes. Su solución no necesariamente será inmediata.

Table 1: Estimación de probabilidad

Para determinar el impacto influyen una serie de factores como es el caso de los agentes amenazadores (¿Quién realiza el ataque?, ¿qué habilidades técnicas tiene?, ¿qué motivaciones tiene?, ¿qué recursos necesita?, ¿qué tamaño tiene?) y las vulnerabilidades (¿Qué facilidad de descubrimiento tiene?, ¿qué facilidad de explotación?, ¿qué tan conocida es?, ¿qué tan probable es que se detecte?).

- Estimar el impacto:

Cuando una amenaza se materializa, se consideran dos tipos de impacto, uno que repercute en la pérdida de confidencialidad, integridad, disponibilidad y trazabilidad, denominado impacto técnico; y otro, en el daño económico, de imagen, de no cumplimiento y de violación a la privacidad, denominado impacto en el negocio.

- Determinar la severidad del riesgo:

Para determinar la severidad del riesgo, se deben considerar los valores de probabilidad de la ocurrencia de la amenaza y del impacto generado sobre el negocio.

Niveles de probabilidad e impacto	
Alto	6 – 9
Medio	3 - <6
Bajo	1-2

Table 2: Niveles de probabilidad e impacto

- Cálculo de Probabilidad: Se asigna un valor a cada uno de los factores de la probabilidad definidos anteriormente.

Threat Agent factors				Vulnerability			
Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrussion detection
5	2	7	1	3	6	9	2
Overall likelihood=4.375 (MEDIUM)							

Table 3: Cálculo de probabilidad

- Cálculo del Impacto: A continuación se realiza el mismo proceso con los factores relacionados con el impacto definidos con anterioridad.

Technical Impact				Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Accountability	Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8	1	2	1	5
Overall technical impact=7.25 (HIGH)				Overall business impact=2.25 (LOW)			

Table 4: Cálculo de impacto

Con los valores definidos, logramos obtener el resultado de la severidad de riesgo, que dado el ejemplo se consideraría un nivel de riesgo alto (probabilidad=medio – impacto=alto) si se contempla el impacto técnico y un nivel bajo (probabilidad=medio – impacto=bajo) si le damos importancia al impacto en el negocio.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	None	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Table 5: Severidad de riesgo

- Priorizar planes de acción:

Una vez que se han clasificado los riesgos de la aplicación, el siguiente paso es desarrollar una lista de priorización para dar solución inmediata a los riesgos identificados con prioridad ALTA.

- Personalizar el modelo de clasificación de riesgos:

El siguiente y último paso es personalizar el modelo de clasificación de riesgos para las aplicaciones de negocio de tu propia organización, ya que esto ayudará a concienciar a las personas de la empresa sobre qué es un riesgo grave, ahorrando mucho tiempo y discusiones para poder aplicar los controles necesarios para mitigarlos.

Para llevarlo a cabo es necesario identificar los factores de riesgo que sean representativos para el negocio en específico y personalizarlos para hacerlo más eficaz y acorde a los procesos reales del negocio.

1.4 Planificación del Trabajo [4]

Para el desarrollo de este trabajo se ha realizado el siguiente diagrama de Gantt en el cual se describen los hitos de cada PEC, las tareas a realizar en cada una de ellas y la planificación de cada tarea.

Figure 2: Diagrama de Gantt

Los recursos utilizados para la elaboración del proyecto:

- Webs
- Asignaturas cursadas en el Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC).

1.5 Breve sumario de productos obtenidos

Al finalizar este proyecto se contará con los siguientes documentos generados:

- Plan de trabajo a realizar: relación de tareas a realizar, fecha de comienzo, duración y relación entre ellas.

- Memoria técnica del proyecto donde se incluye el análisis realizado de los 10 riesgos Top 10 de OWASP de IoT, el análisis de las vulnerabilidades asociadas con sus respectivas pruebas y las mejores prácticas a llevar a cabo para cada uno de los riesgos definidos.

- Video de presentación donde se describirá el trabajo realizado.

1.6 Breve descripción de los otros capítulos de la memoria

El trabajo de final se máster se ha dividido en tres fases importantes teniendo como guía la metodología OWASP de IoT.

FASE 1. Análisis de riesgos y amenazas

En esta primera fase se ha buscado hacer una descripción de los riesgos a los que se exponen los diferentes dispositivos, haciendo mención a las amenazas e impacto que puede sufrir una organización.

FASE 2. Vulnerabilidades asociadas

En la siguiente fase, entraremos a detalle en las vulnerabilidades asociadas a los riesgos descritos en la fase anterior. Se dan una serie de pautas a revisar para determinar si los controles implementados son suficientes o por el contrario están expuestos a dichas vulnerabilidades. Aqui se podrán diferentes ejemplos de ataques.

FASE 3. Mejores prácticas

En esta última fase, se datallarán las mejores prácticas a llevar a cabo para no estar expuesto a las vulnerabilidades descritas anteriormente.

2. OWASP IoT TOP 10

Los dispositivos de IoT, como ya se ha comentado anteriormente, son aquellos que tienen disponibilidad de red y que poseen tecnología integrada, lo que les permite interactuar entre sí y con el entorno. Debido a la gran cantidad y variedad de dispositivos, el IoT se ha convertido en un objetivo atractivo para los hackers o cibercriminales. Actualmente, los usuarios de dispositivos IoT deben ser conscientes de los riesgos a los que se enfrentan y qué hacer para protegerse.

2.1 Riesgos y amenazas de IoT [3]

Tomando como base la metodología de medición del riesgo de OWASP y la OWASP IoT Top 10, la cual indica cuáles son los 10 principales problemas de seguridad asociados con dispositivos del Internet de las Cosas (IoT), pasamos a analizar cada uno de los riesgos Top 10 asociados a IoT.

2.1.1 Uso de contraseñas débiles o en texto plano

Nos encontramos ante el riesgo número uno para los dispositivos IoT de los usuarios. El constante crecimiento del ecosistema de los dispositivos IoT implica mayores puntos de conexión y más contraseñas que manejar y recordar. El uso de contraseñas débiles, predeterminadas, disponibles de manera pública o fáciles de adivinar mediante ataques de fuerza bruta, así como los backdoors en firmware o el cliente de software, permiten obtener acceso no autorizado a los sistemas.

La mayoría de las aplicaciones web usan hoy en día open source o software comercial que es instalado en los servidores con la configuración mínima por el servidor administrador. Una vez que las aplicaciones son instaladas, no están bien configuradas y las contraseñas que se otorgan para la autenticación y configuración inicial están definidas por defecto y nunca son modificadas. Estas contraseñas por defecto, conocidas por los atacantes, son usadas para obtener acceso no autorizado a dichas aplicaciones.

El atacante, ya sea un usuario interno o externo, usa las contraseñas débiles, los mecanismos de recuperación de contraseñas inseguros, la poca protección que hay de las contraseñas o la falta de control de acceso, para acceder a una interfaz o sistema particular.

El impacto que tiene este acceso no autorizado por un usuario malintencionado es la pérdida o corrupción (alteración, eliminación, modificación, etc.) de información, denegación de acceso así como comprometer el dispositivo y/o las cuentas de usuario. Cualquier usuario que tenga acceso a las diferentes interfaces (web, mobile, etc.) podría llevar a cabo un ataque de denegación de servicio (DDoS). De igual manera, el impacto a nivel de negocio sería elevado, afectándole de manera económica e incluso dañando su reputación.

Agentes amenazantes	Vectores de ataque	Debilidades de seguridad		Impacto técnico	Impacto en el negocio
Usuarios internos y/o externos	Explotabilidad MEDIO	Frecuencia COMUN	Detectabilidad FACIL	ALTO	ALTO

Table 6: Resumen riesgo Top 10 - 1

2.1.2 Uso de servicios de red inseguros.

Cuando un atacante intenta comprometer un dispositivo conectado a IoT, la primera superficie de ataque que busca es la debilidad en el modelo de comunicación de la red y en los servicios red que se ejecutan en el dispositivo. El uso de servicios de red inseguros o innecesarios corriendo en el dispositivo, sobre todo en aquellos expuestos a Internet, pueden comprometer la confidencialidad, autenticidad o disponibilidad de la información o pueden permitir el control no autorizado de dicho dispositivo de manera remota.

El usuario malintencionado, ya sea interno o externo, intentará explotar una serie de vulnerabilidades, usando las debilidades del servicio de red, para capturar credenciales de inicio de sesión, tokens u otros identificadores para lograr identificar el dispositivo que desea atacar. Un servicio de red inseguro es susceptible a recibir ataques de buffer overflow o incluso ataques de denegación de servicio dejando el dispositivo inaccesible para el usuario.

El impacto de que esta amenaza se llegue a materializar es la pérdida de información sensible, la denegación de servicio o incluso la apertura de ataques a otros dispositivos. A nivel de negocio, la denegación de servicio de algún dispositivo podría crearle ciertos problemas de interrupción de operaciones.

Agentes amenazantes	Vectores de ataque	Debilidades de seguridad		Impacto técnico	Impacto en el negocio
Usuarios internos y/o externos	Explotabilidad MEDIO	Frecuencia POCO COMUN	Detectabilidad MEDIA	MEDIO	MEDIO

Table 7: Resumen riesgo Top 10 - 2

2.1.3 Uso de interfaces inseguras

Existen problemas de seguridad en interfaces web, móviles, en la nube, o API de back-end en ecosistemas que están fuera de los dispositivos, que permiten que tanto los dispositivos como ciertos componentes relacionados puedan ser comprometidos.

Para solucionar estos problemas, es necesario que exista un mecanismo para autenticar y autorizar el dispositivo. Al garantizar una autenticación con el punto final, se demuestra que cada dispositivo tiene permiso para comunicarse con el proveedor de servicios de IoT. Siempre que los servicios de back-end se comuniquen con un dispositivo IoT, podrán diferenciar entre un punto final válido y un clon forzando al punto extremo a autenticarse.

Los atacantes usan credenciales débiles, la falta de cifrado en el transporte, la falta de autenticación y la falta de bloqueo de cuentas, para acceder a datos y controles a través de la interfaz móvil, web o Internet. Las interfaces inseguras son fáciles de descubrir, por ejemplo identificando

secuencias de cross-site scripting, identificando si el certificado SSL está en uso o utilizando el mecanismo de restablecimiento de contraseñas, para identificar cuentas válidas que pueden conducir a la enumeración de cuentas.

La falta de seguridad en las diferentes interfaces puede provocar la pérdida o corrupción de datos, la denegación de acceso e incluso la toma de control completa del dispositivo. El impacto presentado afectaría la integridad, confidencialidad y disponibilidad del negocio, así como su imagen o reputación.

Agentes amenazantes	Vectores de ataque	Debilidades de seguridad		Impacto técnico	Impacto en el negocio
Usuarios internos y/o externos	Explotabilidad MEDIO	Frecuencia COMUN	Detectabilidad FACIL	ALTO	ALTO

Table 8: Resumen riesgo Top 10 – 3

2.1.4 La falta de un mecanismo seguro de actualización de firmware

El software no autorizado y las actualizaciones de firmware son un vector de amenaza importante para los ataques cibernéticos de IoT. La falta de un sistema sencillo para actualizar el dispositivo de manera segura ya sea la falta de validación del firmware en el dispositivo, la falta de seguridad en el envío (tránsito no cifrado), la falta de mecanismos que permitan evitar volver un paso hacia atrás, o la falta de notificaciones acerca de cambios de seguridad debido a las actualizaciones, pueden tener consecuencias físicas que resultan en la pérdida de datos, así como poner en duda la reputación de la empresa.

Los dispositivos deberían de poder actualizarse cuando una vulnerabilidad es descubierta, además las actualizaciones de software o firmware pueden ser inseguras si los archivos actualizados y la conexión de red a la que se entregan no están protegidos, así como si contiene datos confidenciales codificados como credenciales.

Estos problemas de seguridad son fáciles de descubrir si se realiza una inspección del tráfico de red durante la actualización, para verificar el cifrado o bien se inspecciona el archivo de actualización en busca de información relevante.

La falta de un mecanismo seguro para realizar las actualizaciones podría comprometer los datos de usuario, el control del dispositivo e incluso provocar ataques sobre otros dispositivos a través de cualquier usuario que tenga acceso al dispositivo o a la red donde éste reside. Además, un usuario malintencionado que obtenga acceso al servidor de actualizaciones podría comprometer de igual manera tanto los datos como los dispositivos.

Existen tres requisitos críticos de seguridad para entregar actualizaciones de forma segura a los dispositivos de IoT que deberían de llevarse a cabo:

- Asegurar el acceso a las actualizaciones.
- Verificar la fuente de las actualizaciones.
- Verificar la integridad de las actualizaciones.

Agentes amenazantes	Vectores de ataque	Debilidades de seguridad		Impacto técnico	Impacto en el negocio
Usuarios internos y/o externos	Explotabilidad DIFICIL	Frecuencia COMUN	Detectabilidad FACIL	ALTO	ALTO

Table 9: Resumen riesgo Top 10 – 4

2.1.5 Uso de librerías inseguras o desactualizadas

El uso de componentes/librerías de software obsoletas y/o inseguras, podrían permitir que el dispositivo sea comprometido. Esto incluye personalizaciones inseguras de la plataforma del sistema operativo y el uso de software de terceras partes o componentes de hardware de una cadena de suministro comprometida.

El hecho de usar componentes inseguros o desactualizados implica que tienen vulnerabilidades, las cuales el atacante identifica a través de un escaneo o análisis manual para poder llevar a cabo el ataque. Un usuario malintencionado se aprovecha de estas vulnerabilidades para acceder al sistema operativo, tomar el control de los dispositivos y acceder a los datos.

Mantener los componentes con las últimas actualizaciones evita estas brechas de seguridad y la posibilidad de que el ataque se lleve a cabo.

El posible robo o alteración de los datos así como que los dispositivos se vean comprometidos, afectan a la integridad, confidencialidad y disponibilidad del negocio, además de dañar su imagen y violar la privacidad.

Agentes amenazantes	Vectores de ataque	Debilidades de seguridad		Impacto técnico	Impacto en el negocio
Usuarios internos y/o externos	Explotabilidad MEDIO	Frecuencia AMPLIO	Detectabilidad DIFICIL	MEDIO	MEDIO

Table 10: Resumen riesgo Top 10 - 5

2.1.6 Insuficiente protección de la información personal o privada

La información personal del usuario almacenada en el dispositivo o en el entorno al cual se conecta, es utilizada de manera poco segura, inapropiada o sin permiso. Cualquier usuario, ya sea interno o externo, que tenga acceso al dispositivo, a la red a la que está conectado, a la aplicación móvil y/o a la conexión en la nube, puede tener visibilidad de la información personal o privada.

Un atacante o usuario malintencionado se aprovecha de la autenticación insuficiente, la falta de encriptación de transporte o los servicios de red inseguros para ver datos personales que no están protegidos adecuadamente o que se están recolectando innecesariamente. Estos problemas de privacidad se pueden descubrir revisando los datos que se recopilan a medida que el usuario configura y activa el dispositivo. Existen también herramientas automatizadas capaces de buscar patrones específicos de datos que pueden indicar la recopilación de datos personales u otros datos confidenciales.

La recopilación de datos personales junto con la falta de protección de ellos puede comprometer los datos personales de un usuario, violando la privacidad y afectando la confidencialidad del negocio.

Agentes amenazantes	Vectores de ataque	Debilidades de seguridad		Impacto técnico	Impacto en el negocio
Usuarios internos y/o externos	Explotabilidad MEDIO	Frecuencia COMUN	Detectabilidad FACIL	ALTO	MEDIO

Table 11: Resumen riesgo Top 10 - 6

2.1.7 Almacenamiento y transferencia de datos insegura

La protección de los datos es fundamental para la integridad de las aplicaciones de IoT. Estas aplicaciones de alimentación de datos dan como resultado acciones y controles automatizados que pueden tener consecuencias físicas peligrosas. Es esencial que tanto la fuente como el contenido de los datos generados por los dispositivos de IoT estén protegidos y sean verificables, y para ello es necesario que los datos estén cifrados desde la creación hasta su consumo.

La falta de cifrado o control de acceso para datos sensibles que están tanto en reposo, en tránsito o durante su procesamiento, dentro de la red de redes, permite a los usuarios, ya sean internos o externos, que tengan acceso a la red a la cual está conectado el dispositivo, utilizar esta falta de protección para ver toda la información que pasa tanto por la red local como por Internet.

Se podría considerar la falta de cifrado de los datos en una red local, ya que el tráfico de dicha red no es visible para todo el mundo. Pero si se trata de una red inalámbrica interna, una mala configuración de ésta podría dar visibilidad del tráfico a cualquier persona dentro del alcance de dicha red. Para una protección de la transferencia de los datos adecuada, es necesario realizar una buena implementación del cifrado de transporte como TLS (Transport Layer Security).

El impacto que conlleva el almacenamiento y transferencia de datos no cifrados es la pérdida de dichos datos, ya sea por robo, modificación, alteración o eliminación, y dependiendo de los datos expuestos podríamos hablar incluso del compromiso del dispositivo y de las cuentas de los usuarios. Esto supone un alto impacto al negocio, ya que por un lado el robo de cierta información implica una violación a la privacidad, pudiendo comprometerlos financieramente, así como perjudicar su imagen.

Agentes amenazantes	Vectores de ataque	Debilidades de seguridad		Impacto técnico	Impacto en el negocio
Usuarios internos y/o externos	Explotabilidad MEDIO	Frecuencia COMUN	Detectabilidad FACIL	ALTO	ALTO

Table 12: Resumen riesgo Top 10 - 7

2.1.8 La falta de gestión de dispositivos

La falta de soporte de seguridad en dispositivos lanzados a producción, incluyendo la gestión de activos, gestión de actualizaciones, desarmado seguro, monitoreo de sistemas y capacidades de respuesta, permite a usuarios

con acceso al dispositivo, ya sea intencionadamente o de manera accidental, acceder a los datos y/o controles del dispositivo.

No contar con los conocimientos necesarios conlleva tener una configuración de seguridad insuficiente del dispositivo. Que no se disponga de la capacidad para alterar los controles de seguridad podría derivar en una pérdida de datos o que de manera intencionada o accidental, el dispositivo quede comprometido.

El atacante utiliza la falta de permisos granulares para acceder a datos o controles en el dispositivo, así como la falta de opciones de cifrado y la falta de opciones de contraseña, para realizar otros ataques que puedan comprometer el dispositivo y/o los datos. Los datos podrían ser robados y/o alterados (modificados, eliminados, etc.) afectando la integridad y confidencialidad del negocio, así como la disponibilidad en caso de perder el control de los dispositivos.

Agentes amenazantes	Vectores de ataque	Debilidades de seguridad		Impacto técnico	Impacto en el negocio
Usuario con acceso al dispositivo	Explotabilidad MEDIO	Frecuencia COMUN	Detectabilidad FACIL	MEDIO	MEDIO

Table 13: Resumen riesgo Top 10 – 8

2.1.9 Uso de parámetros por defecto inseguros

Los dispositivos o sistemas lanzados con configuraciones por defecto poco seguras o sin la posibilidad de hacer más seguro al sistema mediante la aplicación de restricciones a partir de cambios en la configuración, hacen posible que los atacantes accedan a cuentas de usuario por defecto, archivos y directorios desprotegidos, entre otros, para posteriormente poder obtener acceso a los datos y/o controles de los dispositivos.

En muchas ocasiones una configuración incorrecta de seguridad, el uso de cuentas o configuraciones predeterminadas, servicios innecesarios u opciones heredadas, hacen fácil el acceso no autorizado para usuarios malintencionados pudiendo provocar un completo compromiso del sistema.

El impacto que conlleva este uso de parámetros por defecto inseguros es la posibilidad de comprometer el dispositivo en sí y cualquier dato de importancia almacenado en él. A nivel de negocio, el impacto es alto, ya que el acceso a la información implica la posible pérdida, robo, alteración (modificación, eliminación, etc.) de ella, así como la pérdida de control del dispositivo, que aunado a la frecuencia con la que ocurre y la facilidad a la hora de detectarlo, afectaría a la confidencialidad, integridad y disponibilidad.

Agentes amenazantes	Vectores de ataque	Debilidades de seguridad		Impacto técnico	Impacto en el negocio
Usuario con acceso	Explotabilidad MEDIO	Frecuencia AMPLIA	Detectabilidad FACIL	MEDIO	ALTO

Table 14: Resumen riesgo Top 10 – 9

2.1.10 Falta de seguridad física en los dispositivos

El hecho de que falten medidas que permitan robustecer los dispositivos desde el punto de vista físico, permite que potenciales atacantes lleguen a información sensible que podría ser de utilidad para un futuro ataque remoto o para tomar control local del dispositivo.

Cualquier usuario que tenga acceso físico al dispositivo puede ser un atacante, que a través de un USB, una tarjeta SD o cualquier otro dispositivo de almacenaje, acceda al sistema operativo o a cualquier dato relevante almacenado en el dispositivo. El aprovechamiento de las debilidades de seguridad en puertos USB o puertos externos, hace que usuarios malintencionados puedan acceder al dispositivo utilizando funciones destinadas a la configuración o al mantenimiento.

El impacto que conlleva esta falta de seguridad física en los dispositivos es la posibilidad de comprometer el dispositivo en sí y cualquier dato de importancia almacenado en él. A nivel de negocio, el impacto también es alto, ya que el acceso a la información implica la posible pérdida, robo, alteración (modificación, eliminación, etc.) de ella, así como la pérdida de control del dispositivo, lo que afectaría a la confidencialidad, integridad y disponibilidad.

Agentes amenazantes	Vectores de ataque	Debilidades de seguridad		Impacto técnico	Impacto en el negocio
Usuario con acceso físico	Explotabilidad MEDIO	Frecuencia COMUN	Detectabilidad MEDIO	ALTO	ALTO

Table 15: Resumen riesgo Top 10 - 10

2.2. Vulnerabilidades asociadas a IoT [3]

Una vez definidos y analizados cada uno de los riesgos Top 10 asociados a IoT, vamos a realizar un estudio sobre las vulnerabilidades asociadas a dichos riesgos. Para ello se llevarán a cabo una serie de pruebas con las cuales se obtendrán evidencias para verificar que tan eficientes son los controles implementados, así como medir el riesgo real del sistema.

2.2.1 Uso de contraseñas débiles o en texto plano

Para verificar si los controles implementados para el uso de contraseñas débiles o en texto plano son eficientes, es necesario llevar a cabo las siguientes revisiones:

- Intentar usar contraseñas débiles como “1234” o “girl” es una manera rápida y fácil de determinar si la política de contraseña es suficiente en todas las interfaces.
- Revisar el tráfico de la red para determinar si las credenciales se transmiten en texto claro.
- Revisar los requisitos en torno a los controles de contraseña, como la complejidad de la contraseña, la verificación del historial de la

contraseña, la caducidad de la contraseña y el restablecimiento forzado de la contraseña para los nuevos usuarios.

- Revisar si se requiere una nueva autenticación para las funciones confidenciales.
- Revisar las distintas interfaces para determinar si las interfaces permiten la separación de roles. Por ejemplo, todas las funciones serán accesibles para los administradores, pero los usuarios tendrán un conjunto más limitado de funciones disponibles.
- Revisar los controles de acceso y probar la escalada de privilegios.

El uso de de una contraseña débil como “1234” o “girl” permiten a un atacante adivinar fácilmente dicha contraseña o capturar las credenciales cuando cruzan la red y descodificarla, ya que las credenciales solo están protegidas mediante la codificación Base64, lo cual permite mediante un ataque de fuerza bruta o de diccionario, obtener la contraseña.

Para obtener la contraseña por fuerza bruta, el cual es un sistema basado en hacer múltiples intentos probando todas las posibles combinaciones hasta dar con la correcta, utilizamos el siguiente script suponiendo que el usuario y la contraseña

```
Username = Irene; Password = girl
```

están poco protegidos cuando se transmiten a través de la red:

```
Authorization: Basic LA2dsdwOhjmNc==
```

Abrir | *script2 ~/Documentos | Guardar

```
#script de ataque de fuerza bruta de 4 caracteres
#!/bin/bash

space1="a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9 0 $ % & / = + @ #"
if [  $# -le 1 ]
then
        echo "Usage: " $0 SALT PASSWORD_CODED
        exit
fi
for i in $space1
do
for j in $space1
do
for k in $space1
do
for l in $space1
do
        variable=$(openssl passwd -crypt -salt "$1" "$i$j$k$l")
        if [ "$variable" = $2 ]
            then
                echo password found: $i$j$k$l
                exit
        fi
done
done
done
done
```

Figure 3: Script ataque fuerza bruta

Este script permite realizar un ataque de fuerza bruta para encontrar una contraseña de cuatro caracteres sobre el alfabeto “a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9 0 $ % & / = + @ #”. El programa tiene como primer parámetro de entrada el "Salt" y como segundo parámetro el hash de la contraseña.

Script	`./script LA LA2dsdwOhjmNc`
Salida	`girl`

```
isalas@debian9:~/Documentos$ time ./script2 LA LA2dsdwOhjmNc
password found: girl
```

Figure 4: Contraseña encontrada

2.2.2 Uso de servicios de red inseguros

Para comprobar si los controles implementados para el uso de servicios de red inseguros son eficientes, es necesario llevar a cabo las siguientes revisiones:

- Revisar el dispositivo en busca de puertos abiertos utilizando un escáner de puertos.
- A medida que se identifican los puertos abiertos, cada uno puede probarse utilizando cualquier número de herramientas automatizadas que buscan vulnerabilidades DDoS, vulnerabilidades relacionadas con servicios UDP y vulnerabilidades relacionadas con desbordamiento de búfer y ataques tipo fuzzing.
- Revisar los puertos de red para asegurarse de que sean absolutamente necesarios y si hay puertos expuestos a Internet mediante UpnP (Universal Plug and Play).

El hecho de tener puertos abiertos a Internet sin el conocimiento del usuario a través de UPnP, permite realizar ataques tipo fuzzing, el cual consiste en enviar datos aleatorios, inválidos y no esperados a las entradas de un programa de ordenador, permitiendo a un atacante deshabilitar el dispositivo completamente a través de un GET HTTP (`GET %s%s%s%s%s%s%s%s%s%s%s%s%s%s HTTP/1.0`) o acceder al dispositivo mediante Internet a través del puerto 80 y/o el puerto 443.

Cuando se establece una comunicación entre dos dispositivos a través del protocolo UpnP [9], uno de ellos puede tener el control del otro sin realizar ningun tipo de autenticación. Uno solicita el URL y el XML de control y el otro se lo envia con el listado de acciones que puede realizar y los parámetros que espera. Al no haber ningun mecanismo de autenticación en dicha convesación, un atacante puede aprovechar esa falta de seguridad para controlar dichos dispositivos e incrementar sus oportunidades de ataque, por ejemplo abriendo puertos.

Figure 5: Intercambio de paquetes en UPnP

Así se ve el diálogo a través de Wireshark, entre dos dispositivos mediante del protocolo UPnP, donde se intercambian información para el control de uno de ellos.

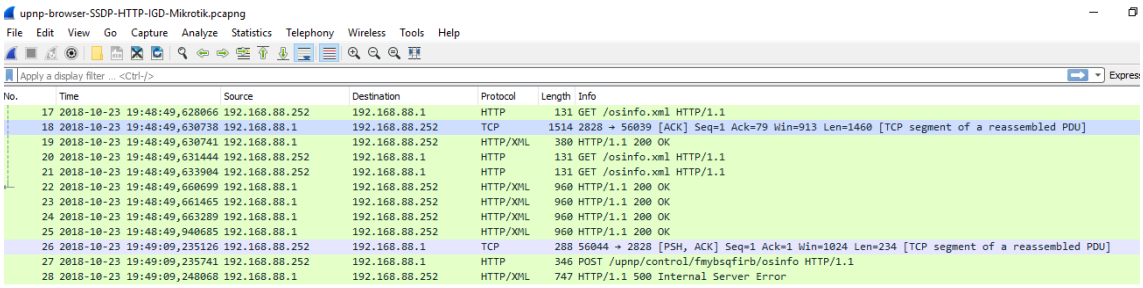

Figure 6: Comunicación UPnP Wireshark

2.2.3 Uso de interfaces inseguras

Para verificar si los controles implementados para el uso de interfaces (web, nube, móvil) inseguras son eficientes, es necesario llevar a cabo las siguientes revisiones:

- Determinar si el nombre de usuario y la contraseña predeterminados se pueden cambiar durante la configuración inicial del producto.
- Determinar si una cuenta de usuario específica se bloquea después de 3 a 5 intentos de inicio de sesión fallidos.
- Determinar si las cuentas válidas se pueden identificar mediante mecanismos de recuperación de contraseña o nuevas páginas de usuario.
- Revisar la interfaz en busca de problemas como la creación de scripts entre sitios, la falsificación de solicitudes entre sitios y la inyección de SQL.
- Revisar todas las interfaces de la nube en busca de vulnerabilidades (interfaces API e interfaces web basadas en la nube).

- Revisar si las credenciales están expuestas mientras están conectadas a redes inalámbricas.
- Revisar si hay disponibles dos opciones de autenticación.

Hay interfaces, como es el caso de la interfaz web, que muestra la funcionalidad de "*contraseña olvidada*", la cual informa a un posible atacante de que al ingresar a una cuenta no válida, la cuenta no existe. Una vez que se identifican las cuentas válidas, es cuestión de tiempo que el atacante identifique la contraseña si no existen controles de bloqueo de cuenta.

Si ingresamos una cuenta y una contraseña aleatorias en el sistema de autenticación:

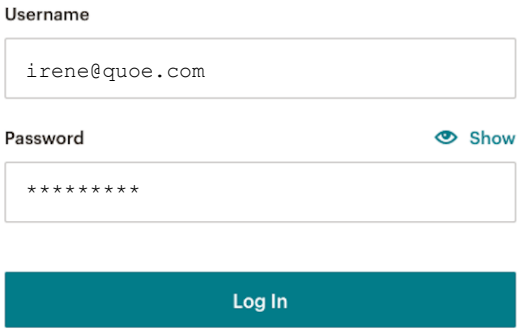

Figure 7: Cuenta no existe

y la cuenta no es válida, el sistema nos arroja el siguiente mensaje:

```
Account irene@quoe.com does not exist.
```

De igual manera, se podría averiguar si la cuenta es válida a través del restablecimiento de contraseña.

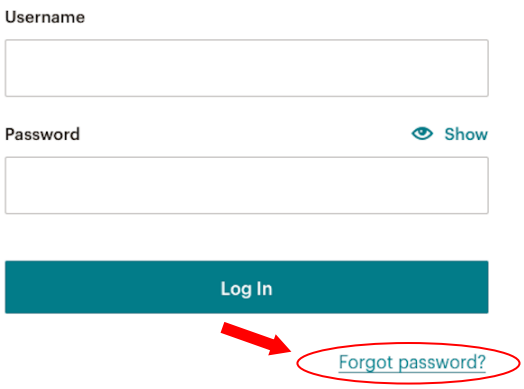

Figure 8: Restablecer contraseña

Al intentar restablecer la contraseña, se pedirá la cuenta para enviar un link para poder reestablecerla.

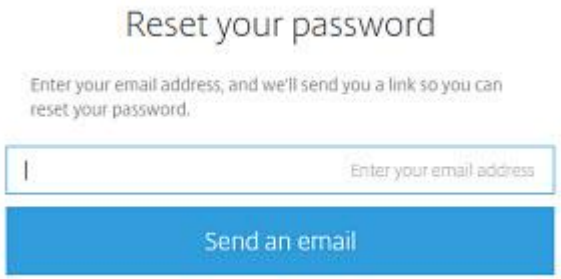

Figure 9: Restablecer contraseña / cuenta no existe

En caso de que la cuenta no sea válida, aparecerá el siguiente mensaje:

```
Password Reset "That account does not exist."
```

De esta manera el atacante podrá determinar de manera sencilla si una cuenta es válida o no. Si además, el nombre de usuario y la contraseña están mal protegidos cuando se transmiten a través de la red:

```
Authorization: Basic S2ZjSDFzYkF4ZzoxMjM0NTY3
```

el atacante también será capaz de capturar las credenciales cuando cruzan la red y decodificarlas, como se ha comentado en el punto 1, ya que las credenciales solo están protegidas mediante la codificación Base64.

También una interfaz web puede ser susceptible a un ataque de cross-site scripting (XSS). Para realizar este ataque, introducimos el siguiente código Javascript que deseamos ejecutar entre dos etiquetas HTML:

```
http://192.168.144.178/xss/example1.php?name=<script>alert(
"Hola colega estas siendo atacado!");</script>
```

Este ataque mostrará un popup en la página web con el mensaje que hemos querido introducir, demostrando que es vulnerable a XSS.

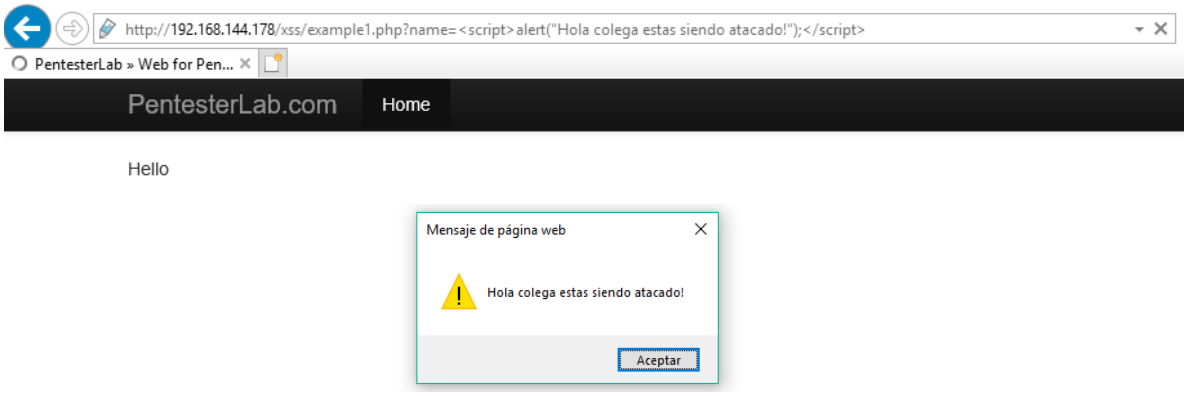

Figure 10: Ataque XSS

2.2.4 La falta de un mecanismo seguro de actualización de firmware

Los dispositivos deben tener la capacidad de actualizar y realizar actualizaciones regularmente. Para comprobar si los controles implementados para la falta de un mecanismo seguro de actualización son eficientes, es necesario llevar a cabo las siguientes revisiones:

- Utilizar una herramienta de edición hexadecimal para revisar el archivo de actualización en sí mismo y así poder detectar la exposición de información confidencial en formato legible por personas.
- Revisar la actualización del archivo de producción para el cifrado adecuado utilizando algoritmos aceptados.
- Revisar la actualización del archivo de producción para asegurar que esté correctamente firmada.
- Revisar el método de comunicación utilizado para transmitir la actualización. Revisar el servidor de actualización en la nube para garantizar que los métodos de encriptación de transporte estén actualizados y configurados correctamente y que el servidor en sí no sea vulnerable.
- Revisar el dispositivo para la validación adecuada de los archivos de actualización firmados.

Cuando se va a realizar una actualización, el archivo de actualización se envía a través del protocolo HTTP (Hypertext Transfer Protocol):

```
http://www.xyz.com/update.bin
```

Si el archivo de actualización no está cifrado, implica que se pueden ver los datos y que éstos son legibles para los seres humanos:

```
�v�ñ]��Ü��Qw�û]��˜3DP�Ö�∂]��˜3DPadmin.htmadvanced.
htmalarms.htm
```

Dada esta situación, un atacante podría capturar el archivo de actualización, ver su contenido e incluso realizar modificaciones en él.

2.2.5 Uso de librerías inseguras o desactualizadas

Para confirmar si los controles implementados para el uso de librerías inseguras o desactualizadas son eficientes, es necesario llevar a cabo las siguientes revisiones:

- Conocer las versiones de todos los componentes que se utilizan (tanto del lado del cliente como del servidor).
- Revisar si el software es vulnerable, posee soporte o se encuentra desactualizado (sistema operativo, servidor web o de aplicaciones, DBMS, APIs y todos los componentes, ambientes de ejecución y bibliotecas).

- Analizar los componentes periódicamente y realizar un seguimiento de los boletines de seguridad de los componentes utilizados.
- Parchear o actualizar la plataforma subyacente, frameworks y dependencias, con un enfoque basado en riesgos (semanalmente).
- Asegurar la configuración de los componentes correctamente.

Aunque los dispositivos de Internet de las Cosas (IoT) son imposibles o muy dificiles de actualizar, la importancia de éstas actualizaciones puede ser enorme. Tal es el caso de los dispositivos biomédicos [5], donde si un equippo está desactualizado y es atacado por esta razón puede atentar contra la vida del paciente.

Existen herramientas automáticas que ayudan a los atacantes a descubrir sistemas mal configurados o desactualizados, como es el caso del motor de búsqueda *Shodan [12]*, el cual ayuda a descubrir dispositivos que aún son vulnerables a *Heartbleed [7]* (vulnerabilidad grave en la biblioteca de software criptográfico OpenSSL), la cual fue parcheada en abril del 2014 y que permite a un atacante leer la memoria de los sistemas protegidos por las versiones vulnerables del software OpenSSL, pudiendo extraer datos de la base de datos que contienen nombres de usuario, contraseñas y otro tipo de información confidencial.

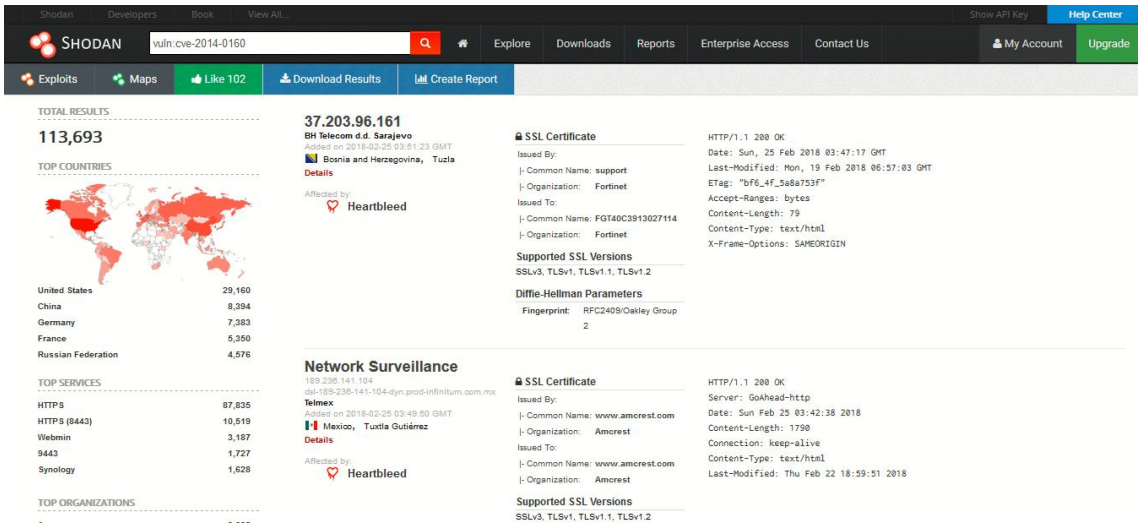

Figure 11: Vulnerabilidad CVE-2014-0160 (Shodan)

2.2.6 Insuficiente protección de la información personal o privada

Para verificar si los controles implementados para la insuficiente protección de la información personal o privada son eficientes, es necesario llevar a cabo las siguientes revisiones:

- Identificar todos los tipos de datos que están siendo recopilados por el dispositivo, su aplicación móvil y cualquier interfaz de nube.
- El dispositivo y sus diversos componentes solo deben recopilar lo necesario para realizar su función.

- La información de identificación personal puede estar expuesta cuando no se cifra correctamente mientras está en reposo en medios de almacenamiento y durante el tránsito a través de redes.
- Revisar quién tiene acceso a la información personal que se recopila.
- Determinar si los datos recopilados se pueden anular o anonimizar.
- Determinar si los datos recopilados van más allá de lo que se necesita para el correcto funcionamiento del dispositivo (¿Tiene el usuario final una opción para esta recopilación de datos?).
- Determinar si una política de retención de datos está en su lugar.

Si la información sensible, como es la información personal o privada, no cuenta con una protección adecuada, se podrían recopilar datos personales o información financiera como:

Fecha de nacimiento
Dirección de tu casa
Número de teléfono
DNI
Número de tarjeta de débito o crédito
Número de cuenta
Historial clínico
Etc.

Si logramos acceder en una empresa, por ejemplo al departamento de RRHH, gracias a algún tipo de vulnerabilidad como las mencionadas en los puntos 2.2.1 o 2.2.9, y existe un archivo ("*Empleados*") cuya información contenida no está cifrada:

Figure 12: Información empleados

La exposición de cualquiera de estos datos podría conducir a un atacante a llevar a cabo un robo de identidad o un compromiso de las cuentas.

Además, utilizando Shodan [12] podemos realizar la búsqueda de personas, gracias a que muchos proveedores de internet ponen en la configuración del router el nombre del cliente incluso su dirección. Por ejemplo, vamos a buscar por uno de los apellidos más populares en España: `Fernández`.

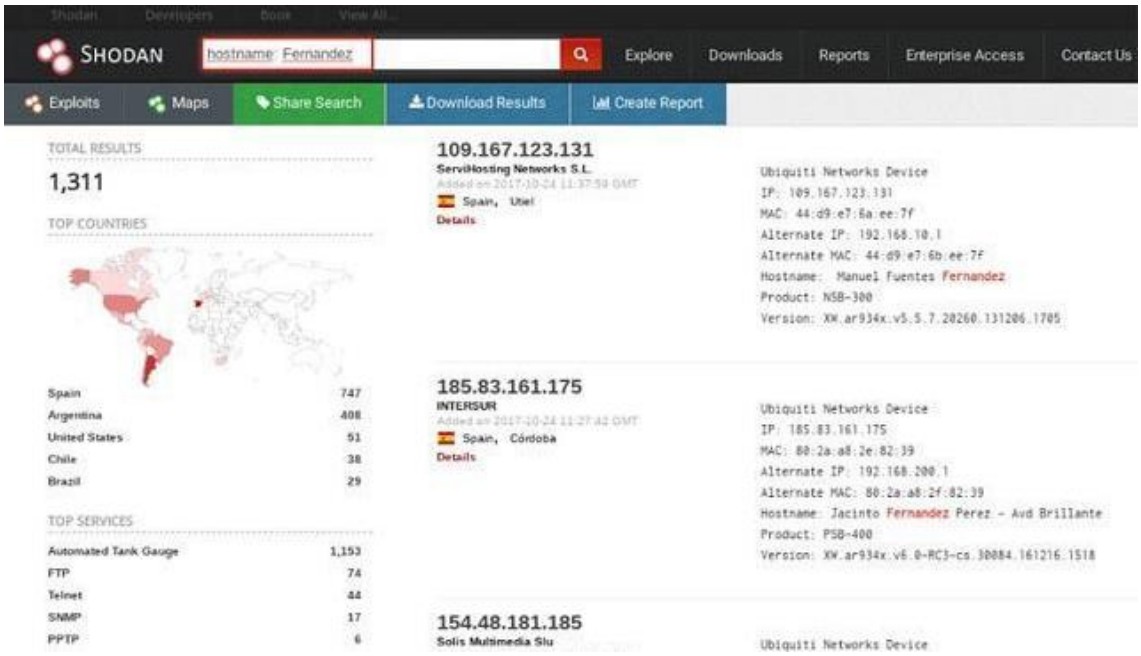

Figure 13: Información personal (Shodan)

2.2.7 Almacenamiento y transferencia de datos insegura

Para comprobar si los controles implementados para el almacenamiento y transferencia de datos insegura son eficientes, es necesario llevar a cabo las siguientes revisiones:

- Revisar el tráfico de red del dispositivo, su aplicación móvil y cualquier conexión a la nube para determinar si se pasa información en texto sin cifrar.
- Revisar el uso de TLS para garantizar que esté actualizado e implementado correctamente.
- Revisar el uso de cualquier protocolo de encriptación para asegurar que sean recomendados y aceptados.

Si por ejemplo usamos la interfaz de la nube, la cual solo usa el protocolo HTTP, `http://www.xyzcloudsite.com`, y al autenticarnos el usuario y la contraseña se transmiten en texto plano a través de la red, ya que la transferencia de datos no es segura:

`http://www.xyzcloud.com/login.php?userid=3&password=girl`

un atacante podría ver la información sensible o los datos confidenciales en claro, debido a la falta de cifrado de transporte.

Otro ejemplo, realizado con la herramienta burp, si no se realiza una redirección automática del puerto 80 al 443 (cifrado) el usuario se autentica a la página por el protocolo sin cifrar y las contraseñas se transmiten en claro por la red. Por este motivo, si el usuario accede a través del protocolo sin cifrar, es posible capturar las credenciales y la cookie de sesión mientras viajan por la red, como se puede ver en la siguiente captura realizada con un proxy web:

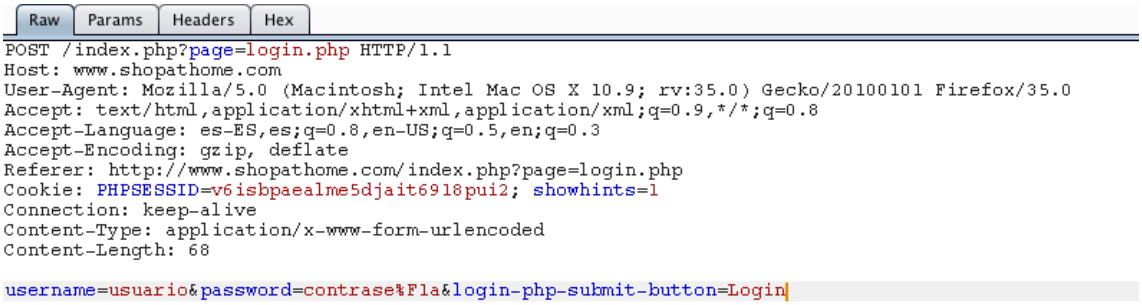

Figure 14: Información sensible viajando sin cifrar

2.2.8 La falta de gestión de dispositivos

Para verificar si los controles implementados para la falta de gestión de dispositivos son eficientes, es necesario llevar a cabo las siguientes revisiones:

- Revisar la interfaz administrativa del dispositivo en busca de opciones para fortalecer la seguridad, como forzar la creación de contraseñas seguras.
- Revisar la interfaz administrativa para la capacidad de separar a los usuarios administradores de los usuarios normales.
- Revisar la interfaz administrativa para las opciones de cifrado.
- Revisar la interfaz administrativa en busca de opciones para habilitar el registro seguro de varios eventos de seguridad.
- Revisar la interfaz administrativa en busca de opciones para habilitar alertas y notificaciones al usuario final para eventos de seguridad.

En el caso de que no haya capacidad para hacer cumplir las políticas de contraseña fuerte, es decir, que tanto los administradores como los usuarios tengan permisos para crear las contraseñas de sus cuentas, o bien que no haya capacidad para habilitar el cifrado de datos cuando están en reposo, permiten a un atacante obtener el acceso a las cuentas de usuario con contraseñas débiles o acceder a los datos en reposo (personales, confidenciales, etc.).

La falta de uso de plataformas de gestión de dispositivos como sophos, azure, etc., facilita al atacante el acceso a información privada o confidencial.

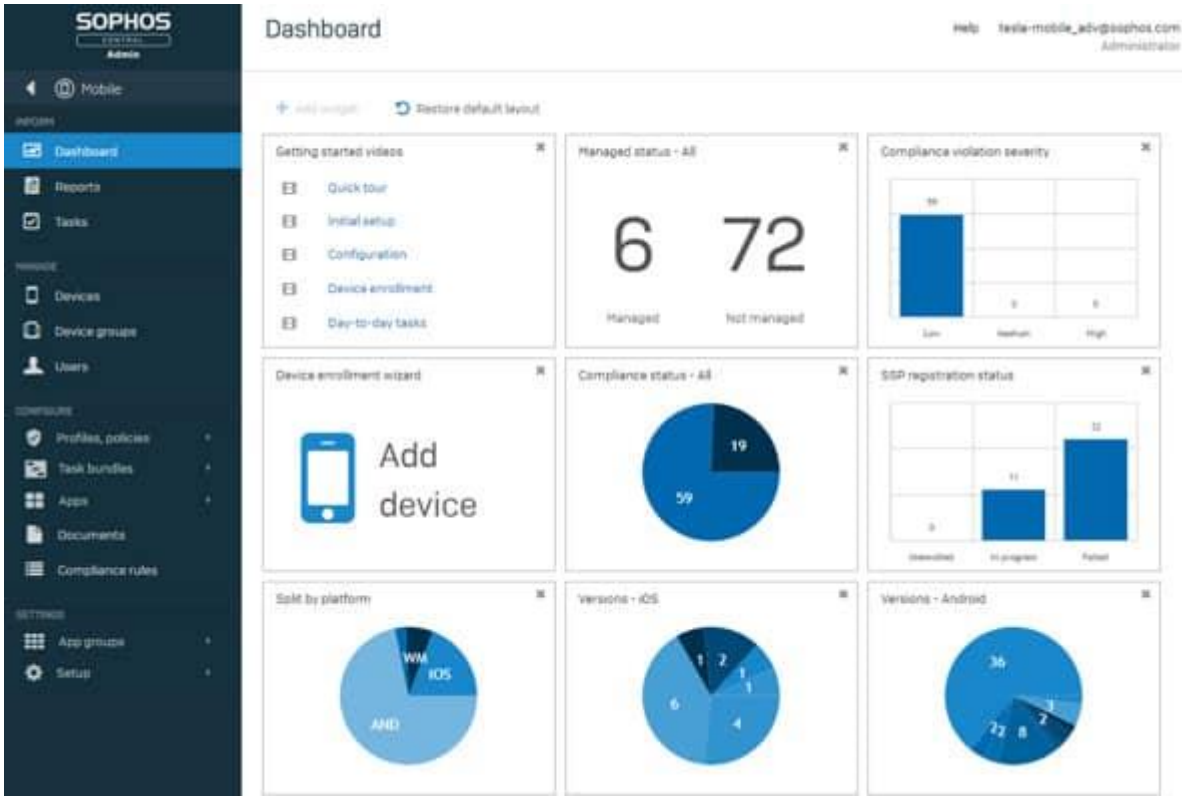

Figure 15: Gestión de dispositivos (Sophos) [13]

2.2.9 Uso de parámetros por defecto inseguros

Para confirmar si los controles implementados para el uso de parámetros por defecto son eficientes, es necesario llevar a cabo las siguientes revisiones:

- Revisar el servicio a desplegar y buscar una configuración suficientemente fuerte (funciones de seguridad desactivadas o mal configuradas).
- Revisar la reutilización de credenciales conocidas o el uso de contraseñas por defecto, débiles o muy conocidas, como “Password1”, “Contraseña1” o “admin/admin”.
- Revisar la instalación de carácterísticas innecesarias (puertos, servicios, páginas, cuentas o servicios).
- Revisar la configuración de los permisos.
- Revisar la existencia de cuentas predeterminadas con sus contraseñas activas y sin cambios.

Un atacante escanea usuarios haciendo uso de listas de contraseñas por defecto para tomar el control de todas las cuentas utilizando esos datos. Si por ejemplo tenemos una cuenta de administrador, donde el usuario es `admin`, y la contraseña es `1234` por defecto, para acceder a la base de datos de una empresa, y un atancante logra entrar, podría acceder a información confidencial de la organización pudiendo comprometerla.

Usamos nuevamente Shodan [12], e introducimos en el buscador `admin+1234`.

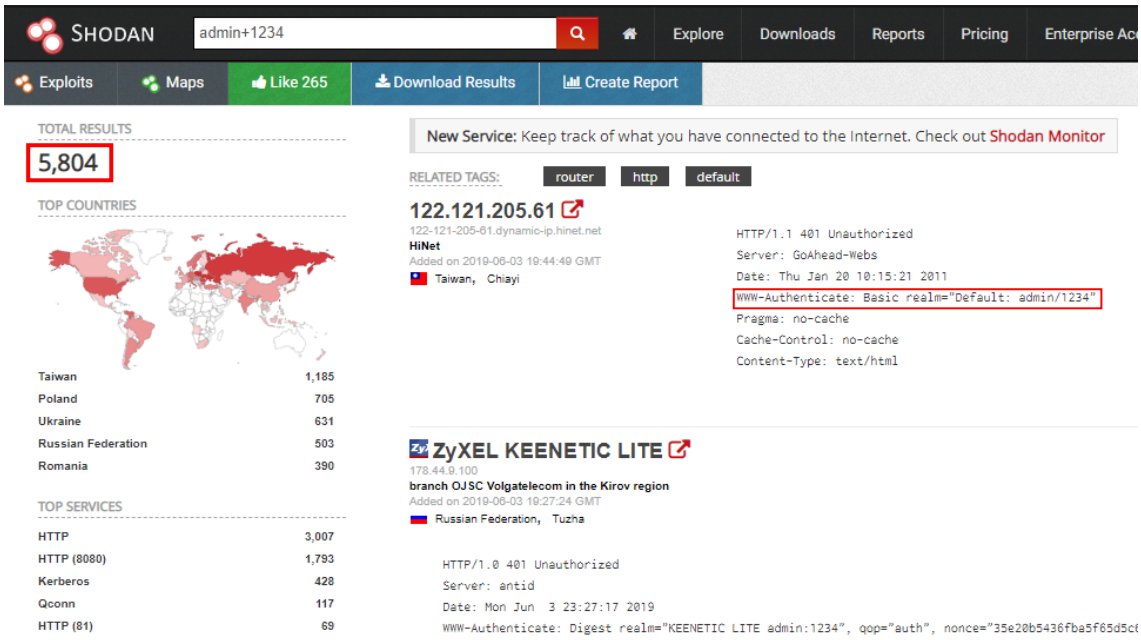

Figure 16: Credenciales por defecto (Shodan)

Esta simple búsqueda nos ha devuelto 5,804 resultados de dispositivos IP cuyas credenciales por defecto son admin/1234. De hecho en la respuesta del dispositivo de la imagen se puede comprobar que dicha información aparece en la línea: `WWW-Authenticate: Basic realm="Default: admin/1234"`. Comprobamos con una de las direcciones IP, la veracidad de esta información:

Figure 17: Comprobación credenciales

**Nota: Por cuestiones de legalidad no se han introducido los datos, pero un atacante sí lo haría y las probabilidades de que el acceso tenga éxito (por desgracia) son muchas.

2.2.10 Falta de seguridad física en los dispositivos

Para verificar si los controles implementados para la falta de seguridad física en los dispositivos son eficientes, es necesario llevar a cabo las siguientes revisiones:

- Revisar la facilidad con que se puede desarmar un dispositivo y acceder o eliminar los medios de almacenamiento de datos.
- Revisar el uso de puertos externos, como el USB, para determinar si se puede acceder a los datos en el dispositivo sin desmontar el dispositivo.
- Revisar la cantidad de puertos físicos externos para determinar si todos son necesarios para la función adecuada del dispositivo.
- Revisar la interfaz administrativa para determinar si se pueden desactivar puertos externos como el USB.
- Revisar la interfaz administrativa para determinar si las capacidades administrativas pueden limitarse solo al acceso local.
- Revisar que el dispositivo cuenta con la espiral electromagnética para evitar el descubriento de la información por variaciones en el campo eléctrico.
- Revisar que el dispositivo cuenta con un chip adicional dedicado exclusivamente al cifrado de la infromación almacenada.

Cuando hacemos uso de dispositivos físicos removibles como es el caso de una tarjeta SD o un USB sin cifrar, corremos el riesgo de que un atacante pueda acceder a ellos, ya sea quitando la tarjeta SD e insertándola en un lector de tarjetas siendo alterada (modificada, copiada, etc.) o incluso acceder al software original del dispositivo a través de un puerto USB, dándole la opción de poder realizar modificaciones o copiar datos específicos.

2.3. Mejores prácticas a llevar a cabo [3]

Tras definir los riesgos, amenazas, y las vulnerabilidades asociadas a dichos riesgos que afectan a los dispositivos y entornos de IoT, necesitamos desarrollar una serie de medidas de protección o acciones a llevar a cabo para mitigarlas. A continuación se indican una serie de recomendaciones a aplicar.

2.3.1 Uso de contraseñas débiles o en texto plano

Para mitigar el uso de contraseñas débiles, predeterminadas, disponibles de manera pública o fáciles de adivinar mediante ataques de fuerza bruta, así como los backdoors en firmware o el cliente de software, permiten obtener acceso no autorizado a los sistemas, es necesario:

- Asegurar que las contraseñas sean fuertes:

    - Utilizar una longitud igual o superior a los 9 dígitos.
    - Si se usan palabras comunes, que sean al menos una combinación de varias, intercalando mayúsculas y minúsculas, con números y símbolos.
    - No usar un patrón del teclado del ordenador o del móvil.
    - Si se usa una contraseña numérica, que no sean números consecutivos o iguales.
    - Los mismo con las letras del abecedario.

- Asegurar el control de acceso granular cuando sea necesario:

    - El control de acceso basado en roles (RBAC) [11] es utilizado en la actualidad por la mayor parte de las empresas con más de 500 empleados. Es muy versátil y contrasta con la rigidez de los métodos tradicionales de control de acceso, que conceden o revocan el acceso de los usuarios objeto por objeto. En RBAC, se pueden añadir, modificar y eliminar roles de forma dinámica a medida que evolucionan las necesidades de la empresa, sin tener que actualizar individualmente los privilegios para cada usuario. Consta de una estructura jerárquica y de una colección de restricciones que se aplican a la asignación de los usuarios a los roles y de los permisos a los roles para poder soportar la “Separación de Deberes” (SOD) que específica el estándar RBAC del NIST.

- Asegurar que las credenciales estén protegidas adecuadamente utilizando métodos de mejora de protección de contraseñas:

    - Por ejemplo en sistemas Linux/Unix, el uso del método “shadow password”. Anteriormente las contraseñas se guardaban cifradas en una carpeta para la cual, todos los usuarios tenían privilegios de lectura (/etc/passwd). Mediante este método, todos los usuarios siguen teniendo privilegios de lectura de esa carpeta, pero las contraseñas se guardan en otra, (/etc/shadow) donde solo tiene privilegios de lectura el administrador del sistema (root). Donde debería aparecer el campo correspondiente a la clave cifrada, no aparece ésta, sino una serie de símbolos que indican a determinados programas, buscar las claves en la nueva carpeta donde solo el root tiene privilegios. La carpeta /etc/shadow, guarda un hash de la carpeta /etc/passwd. Así, a partir de la contraseña se puede calcular el hash, para comprobar que la contraseña de acceso al sistema es correcta, pero no es posible hacerlo de manera inversa. Si un atacante se hiciera con la carpeta /etc/shadow no podría obtener con ella, las contraseñas.

- Asegurar que los mecanismos de recuperación de contraseña sean seguros:

    - Configurar la recuperación de contraseñas a través de un correo alternativo.
    - Configurar la recuperación de contraseñas a través de una pregunta secreta, cuya respuesta no debe estar basada en información verídica y debe ser fácil de recordar por el usuario.

2.3.2 Uso de servicios de red inseguros

Para poder hacer frente al uso de servicios de red inseguros o innecesarios corriendo en el dispositivo, sobre todo en aquellos expuestos a

Internet, que pueden comprometer la confidencialidad, autenticidad o disponibilidad de la información o pueden permitir el control no autorizado de dicho dispositivo de manera remota, se requiere:

- Asegurar que sólo los puertos necesarios estén expuestos y disponibles.
- Asegurar que los servicios no sean vulnerables a desbordamientos de búfer (buffer overflow) y ataques tipo fuzzing.
- Asegurar que los servicios no sean vulnerables a los ataques DDoS que pueden afectar al propio dispositivo u otros dispositivos y/o usuarios en la red local u otras redes.
- Asegurar que los puertos o servicios de red no estén expuestos a Internet a través de UPnP, por ejemplo.
- El tráfico de solicitud de servicio anormal se debe detectar y bloquear en la capa de puerta de enlace de servicio.

2.3.3 Uso de interfaces inseguras

Para solucionar problemas de seguridad en interfaces web, móviles, en la nube, o API de back-end en ecosistemas que están fuera de los dispositivos, que permiten que tanto los dispositivos como ciertos componentes relacionados puedan ser comprometidos, es necesario:

- Asegurar el cambio de contraseña o nombres de usuario predeterminados durante la configuración inicial .
- Asegurar que los mecanismos de recuperación de contraseñas sean robustos y no proporcionen a un atacante información que indique una cuenta válida.
- Asegurar que la interfaz web no sea susceptible a XSS, SQLi o CSRF.
- Asegurar que las credenciales no estén expuestas en el tráfico de la red interna o externa.
- Asegurar que las contraseñas débiles no están permitidas.
- Asegurar el bloqueo de la cuenta después de 3-5 intentos de inicio de sesión fallidos.
- Asegurar que las cuentas de usuario no se puedan enumerar usando funcionalidad como los mecanismos de restablecimiento de contraseña.
- Asegurar que las credenciales no estén expuestas a través de internet o mientras están conectadas a redes inalámbricas
- Implementar la autenticación de dos factores si es posible.
- Detectar o bloquear los requerimientos / intentos anormales.

2.3.4 La falta de un mecanismo seguro de actualización de firmware

Para evitar que un mecanismo inseguro para realizar actualizaciones pueda comprometer los datos de usuario, el control del dispositivo e incluso provocar ataques sobre otros dispositivos a través de cualquier usuario que

tenga acceso al dispositivo o a la red donde éste reside, existen tres requisitos críticos de seguridad que deberían de llevarse a cabo:

- Asegurar el acceso a las actualizaciones.
- Verificar la fuente de las actualizaciones.
- Verificar la integridad de las actualizaciones.

Además, es necesario:

- Asegurar que el dispositivo tenga la capacidad de actualización (muy importante, necesita un mecanismo de actualización seguro).
- Asegurar que el archivo de actualización esté cifrado utilizando métodos de cifrado aceptados.
- Asegurar que el archivo de actualización se transmita a través de una conexión encriptada.
- Asegurar que el archivo de actualización no exponga datos confidenciales.
- Asegurar que la actualización esté firmada y verificada antes de permitir que la actualización se cargue y aplique.
- Asegurar que el servidor de actualizaciones sea seguro.
- Implementar el arranque seguro si es posible (cadena de confianza).

2.3.5 Uso de librerías inseguras o desactualizadas

Para evitar el uso de componentes/librerías de software obsoletas y/o inseguras que podrían permitir que el dispositivo sea comprometido, es necesario implementar los siguientes requisitos:

- Asegurar que los componentes cuentan con última versión instalada.
- Asegurar que los componentes que se utilizan cuentan con soporte.
- Asegurar, mediante diversos análisis, los componentes periodicamente (semanalmente).
- Asegurar la configuración de los componentes correctamente.

2.3.6 Insuficiente protección de la información personal o privada

Para mejorar la protección de la información personal o privada del usuario almacenada en el dispositivo o en el entorno al cual se conecta, es necesario:

- Asegurar que solo se recopilan datos críticos para la funcionalidad del dispositivo.
- Asegurar que cualquier información recopilada no sea de naturaleza confidencial.
- Asegurar que cualquier dato recolectado sea anónimo o no identificado.
- Asegurar que cualquier dato recolectado esté adecuadamente protegido con su correspondiente cifrado.

- Asegurar que el dispositivo y todos sus componentes protejan adecuadamente la información personal.
- Asegurar que solo las personas autorizadas tengan acceso a la información personal recopilada.
- Asegurar límites de retención para los datos recopilados.
- Asegurar que los usuarios finales reciban un "Aviso y elección" si los datos recopilados son más de lo que se esperaría del producto.
- Asegurar el control/autorización de acceso basado en roles a los datos recopilados/analizados.
- Asegurar que los datos analizados no sean identificados.

2.3.7 Almacenamiento y transferencia de datos insegura

Para mejorar la falta de cifrado o control de acceso para datos sensibles que están tanto en reposo, en tránsito o durante su procesamiento, dentro de la red de redes, se requiere lo siguiente:

- Asegurar que los datos se cifren mediante protocolos como TLS mientras se transitan las redes.
- Asegurar que se utilizan otras técnicas de cifrado estándar de la industria para proteger los datos durante el transporte si TLS no está disponible.
- Asegurar que solo se utilizan los estándares de cifrado aceptados y evitar el uso de protocolos de cifrado propietarios.
- Asegurar el cifrado de la carga útil del mensaje.
- Asegurar la clave segura de cifrado handshaking.
- Asegurar la verificación de la integridad de los datos recibidos.

2.3.8 La falta de gestión de dispositivos

La falta de soporte de seguridad en dispositivos lanzados a producción, incluyendo la gestión de activos, gestión de actualizaciones, desarmado seguro, monitoreo de sistemas y capacidades de respuesta, permite a usuarios con acceso al dispositivo, ya sea intencionadamente o de manera accidental, acceder a los datos y/o controles del dispositivo.

- Asegurar la capacidad de separar a los usuarios normales de los usuarios administrativos.
- Asegurar la capacidad de cifrar datos en reposo o en tránsito.
- Asegurar la capacidad de forzar políticas de contraseña fuerte.
- Asegurar la capacidad de habilitar el registro de eventos de seguridad.
- Asegurar la capacidad de notificar a los usuarios finales de eventos de seguridad.

2.3.9 Uso de parámetros por defecto inseguros

Para proteger los dispositivos o sistemas lanzados con configuraciones por defecto poco seguras o sin la posibilidad de hacer más seguro al sistema mediante la aplicación de restricciones a partir de cambios en la configuración, es necesario seguir los siguientes puntos:

- Asegurar que el servicio a desplegar y su configuración son suficientemente fuertes (funciones de seguridad desactivadas o mal configuradas).
- Asegurar el cambio de contraseñas por defecto conocidas como “Password1”, “Contraseña1” o “admin/admin”.
- Asegurar que las características de instalación son las necesarias (puertos, servicios, páginas, cuentas o servicios).
- Asegurar que la configuración de los permisos es la adecuada.
- Asegurar el cambio de contraseñas en cuentas predeterminadas activas.

2.3.10 Falta de seguridad física en los dispositivos

Para robustecer los dispositivos desde el punto de vista físico, es necesario instaurar las siguientes medidas de protección:

- Asegurar que el medio de almacenamiento de datos no se puede quitar fácilmente.
- Asegurar que los datos almacenados se cifran en reposo.
- Asegurar que los puertos USB u otros puertos externos no se puedan usar para acceder maliciosamente al dispositivo.
- Asegurar que el dispositivo no se pueda desmontar fácilmente.
- Asegurar que solo se requieren los puertos externos requeridos, como el USB, para que el producto funcione .
- Asegurar que el producto tenga la capacidad de limitar las capacidades administrativas.
- Asegurar que el dispositivo cuenta con protección para evitar que la información pueda ser descubierta a través de variaciones en el campo electromagnético (espiral metálica).

3. Conclusiones

Con este proyecto se ha querido realizar un estudio de las diferentes amenazas y riesgos que existen actualmente en el ecosistema de IoT, tomando como base la metodología OWASP para IoT.

Tras analizar los principales riesgos descritos por la OWASP, se ha comprobado que la materialización de ellos puede suponer un gran impacto en las organizaciones, afectando tanto a la información que manejan, como a sus funcionalidades, la confianza que depositan los usuarios, la imagen de la organización, y a los ingresos de las compañías.

Se han realizado diferentes pruebas para estudiar las vulnerabilidades asociadas a dichos riesgos, las cuales hay que tener en cuenta para proteger los dispositivos de la red de redes.

Y por último se han dado una serie de pautas o controles a seguir para mitigar los riesgos, amenazas y vulnerabilidades en los dispositivos de IoT.

La planificación del proyecto se ha seguido según lo previsto y tras la finalización se comprueba que ha sido adecuada.

Con toda esta información se considera que se han cumpido los objetivos propuestos para el trabajo aunque quedarían pendientes algunas pruebas más que no se han podido realizar por falta de permisos.

4. Glosario

Internet of Things (IoT): es una red de redes donde una gran cantidad de objetos o dispositivos se alojan y se pueden conectar entre sí.

Amenazas: acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información..

Vulnerabilidad [6]: debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

Riesgo: combinación de la probabilidad de que ocurra un incidente de seguridad al materializarse una amenaza, y la severidad del daño o deterioro que puede causar el incidente.

Probabilidad: estimación de ocurrencia de una amenaza sobre un activo.

Impacto: es las consecuencia de que las amenazas se llegasen a materializar sacando provecho de una vulnerabilidad asociada a un activo.

Integridad: con integridad se quiere decir que la información no ha sido manipulada, alterada, borrada o copiada, ni en el trayecto ni en el origen y que estamos seguros de ello.

Confidencialidad: cuando se habla de confidencialidad se refiere a que sólo pueden acceder a la información privilegiada aquellas personas que tienen autorización para hacerlo.

Disponibilidad: la disponibilidad hace referencia a que la información siempre este disponible cuando los usuarios autorizados la precisen.

Cross-site scripting (XSS): técnica de ataque que permite a una tercera persona inyectar en el sitio web código Javascript o en otro lenguaje similar, evitando medidas de control como la política del mismo origen.

Fuerza bruta: forma de recuperar una contraseña probando todas las combinaciones possibles hasta encontrar aquella que permite el acceso.

Hypertext Transfer Protocol (HTTP): esquema de protocolo usado en la Wold Wide Web. HTTP describe la manera en que un cliente pide datos y como un servidor web responde a esas peticiones.

Secure Socket Layer (SSL): protocolo de clave pública estandar usado para crear túneles cifrados entre dos dispositivos conectados en una red.

Denegación de servicio (DDos): técnica de ataque que consume todos lo recursos disponibles de un sitio web con la intención de que no sea posible

acceder por los usuarios legítimos. Los recursos a comsumir pueden ser tiempo de CPU, memoria, ancho de banda, espacio en disco, etc. Cuando uno de esos recursos alcanza su capacidad completa, el sistema normalmente será inaccesible para la actividad normal de los usuarios.

Open Web Application Security Project (OWASP): comunidad de seguridad informática formada por empresas, organizaciones educativas y particulares de todo mundo, que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías dedicados a determinar y combatir las causas que hacen que el software sea inseguro.

Universal Plug and Play (UPnP) [9]: protocolo que permite el descubrimiento, la conexión y la comunicación directa de dos o más aplicaciones entre sí que se conecten tanto a una red local como a Internet.

Fuzzing [8]: consiste en enviar datos aleatorios, inválidos y no esperados mediante los formularios de entrada de una aplicación buscando alguna vulnerabilidad en ella.

5. Bibliografía

[1] IoT - https://www.domodesk.com/221-a-fondo-que-es-iot-el-internet-de-las-cosas.html,
https://es.semrush.com/blog/iot-internet-cosas-influencia/,
http://www.nunkyworld.com/internet-las-cosas-cambiara-nuestra-vida/,
https://blog.pandorafms.org/es/que-es-el-iot/,
https://www.incibe-cert.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot,
https://es.wikipedia.org/wiki/Internet_de_las_cosas
Fechas: 06-03-2019, 09-03-2019, 10-03-2019

[2] OWASP Risk Rating Management -
https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
https://www.owasp.org/images/9/9c/Riskratingmanagement-170615172835.pdf
https://www.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf
Fechas: 12-03-2019, 14-03-2019, 15-03-2019

[3] Top 10 OWASP IoT -
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
https://www.owasp.org/index.php/Top_10_2014-I9_Insecure_Software/Firmware
https://www.owasp.org/index.php/Top_10_2014-I5_Privacy_Concerns
https://www.owasp.org/index.php/Top_10_2014-I4_Lack_of_Transport_Encryption
https://www.owasp.org/index.php/Top_10_2014-I10_Poor_Physical_Security
https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization
https://www.owasp.org/index.php/Top_10_2014-I3_Insecure_Network_Services
https://www.owasp.org/index.php/Top_10_2014-I6_Insecure_Cloud_Interface
https://www.owasp.org/index.php/Top_10_2014-I7_Insecure_Mobile_Interface
https://www.owasp.org/index.php/Top_10_2014-I1_Insecure_Web_Interface
https://www.owasp.org/index.php/Top_10_2014-I8_Insufficient_Security_Configurability
https://nvisium.com/blog/2019/01/02/internet-of-things-owasp-top-10-2018-released.html
https://www.welivesecurity.com/la-es/2019/01/07/principales-fallos-seguridad-dispositivos-iot/
https://www.owasp.org/index.php/Top_10_2013-A9-Using_Components_with_Known_Vulnerabilities
https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf
https://es.wikipedia.org/wiki/Open_Web_Application_Security_Project
Fechas: del 14-03-2019 al 29-05-2019

[4] Diagrama de Gantt - https://instagantt.com/r#
Fechas: 11-03-2019, 01-04-2019, 29-04-2019

[5] Dispositivos médicos - https://www.welivesecurity.com/la-es/2014/06/02/vulnerabilidades-dispositivos-medicos-que-expuesto-estas/
Fechas: 21-04-2019

[6] Vulnerabilidad - https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
https://hacking-etico.com/2017/04/04/las-principales-vulnerabilidades-web/
Fechas: 10-04-2019, 19-04-2019

[7] Heartbleed - https://blogmexico.comstor.com/la-vulnerabilidad-heartbleed-que-es-y-como-afecta
Fechas: 29-05-2019

[8] Fuzzing - https://openwebinars.net/blog/como-hacer-fuzzing/
https://www.welivesecurity.com/la-es/2012/10/31/detectando-vulnerabilidades-softwar-mediante-fuzzing/
Fechas: 29-05-2019, 03-06-2019

[9] UpnP - https://www.hackplayers.com/2015/09/filet-o-firewall-o-como-el-upnp-de-tu.html
https://es.wikipedia.org/wiki/Universal_Plug_and_Play
Fechas: 29-05-2019, 03-06-2019

[10] Recuperación de contraseñas-
https://www.osi.es/es/actualidad/avisos/2009/01/23/debilidad-en-el-mecanismo-de-recuperaci%C3%B3n-de-contrase%C3%B1-en-el-correo-web
Fechas: 15-05-2019

[11] RBAC - https://arquitecturasoftware.wordpress.com/tag/xacml/
Fechas: 24-05-2019

[12] Shodan - http://blog.svtcloud.com/shodan-usuarios-y-contrasenas-por-defecto/
https://www.shodan.io/home
https://www.shodan.io/search?query=admin%2B1234
https://eltallerdelbit.com/shodan-buscador/#filtros
Fechas: 29-05-2019, 03-06-2019

[13] Sophos -
https://www.google.com/search?q=gestion+de+dispositivos+IoT&tbm=isch&tbs=rimg:CXWMD2EMhOSzIjhZRDvgm2P6TxRhalpzLge16upsrtekfRnu70VReJRAMCyVh4BdPyKntPMnww7UzjEurAjejtywMioSCVlEO-CbY_1pPEZyJbEDcF2WxKhIJFGFqWnMuB7URzKI-gpXdWJwqEgnq6myu16R9GRH59EpIFUzcoSoSCe7vRVF4lEAwEaU1nOYo9YwRKhIJLJWHqF0_1IqcRJuQYzs7aYqEqEgm08yfDDtTOMRHRtTxcoZsQSioSCS6sCN6O3LAyEYS-RvY6bNY1&tbo=u&sa=X&ved=2ahUKEwjtqaGHx87iAhWSoJ4KHd_7DUAQ9C96BAgBEBs&biw=1366&bih=625&dpr=1#imgrc=dYwPYQyE5LOT2M:
Fechas: 03-06-2019