TFM – Seguridad en la Internet de las Cosas (IoT)

Irene Salas Sanz
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Universidad Oberta de Cataluña
11 junio 2019

RESUMEN

Elaboración de un estudio sobre la ciberseguridad en el Internet of Things (IoT), analizando sus amenazas, riesgos y vulnerabilidades.

El trabajo se ha divido en tres fases importantes:

FASE 1. Análisis de riesgos y amenazas

FASE 2. Vulnerabilidades asociadas

FASE 3. Mejores prácticas

Para la realización de este estudio se ha seguido la metodología OWASP de IoT, asi como la metodología OWASP Risk Rating Management para la medición de los riesgos.

Contextualización, justificación y objetivos del trabajo

- Hoy en dia el IoT se ha convertido en un elemento más en nuestra vida cotidiana.
- Integración entre el mundo real y el tecnológico.
- Manejar los dispositivos de manera remota desde cualquier parte del mundo
- Hacer más cómodas nuestras vidas
- Proporcionar seguridad en diversos ámbitos.

Riesgos asociados a la seguridad y privacidad

➢ Objetivos:

- Realizar un estudio sobre los diferentes riesgos y amenazas asociados a IoT.
- Realizar un estudio en profundidad sobre las vulnerabilidades asociadas.
- Realizar una guía sobre las mejores prácticas para estar protegido de los riesgos y amenazas relacionados con IoT

The Open Web Application Security Project (OWASP)

- Comunidad de código abierto (open source) enfocada en la seguridad de aplicaciones web
- OWASP Top 10 – Identifica los riesgos más comunes y críticos

OWASP Top 10

- No es un estándar, es un documento para crear conciencia

Publicaciones

- 2003, 2004, 2007, 2010, 2013, 2017, 2018

Es sobre riesgos, no sólo vulnerabilidades

- Título: “The Top 10 Most Critical Web Application Security Risks”

OWASP top 10 Risk Rating Methodology

- Basado en la metodología OWASP Risk Rating, usada para priorizar el Top 10

OWASP Top 10 Risk Rating Management

Riesgo = Probabilidad x Impacto

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

Cálculo de la probabilidad

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)							

Cálculo del impacto

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)			

OWASP Top 10 Risk Rating Management

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Probabilidad = 4,375 (MEDIUM)
Impacto de negocio = 2,25 (LOW)

Riesgo = LOW

THE OWASP IoT TOP 10 (Edición 2018)

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 de dispositivos
9. Uso de parámetros por defecto inseguros
10. Falta de seguridad física en los dispositivos

1. Uso de contraseñas débiles o en texto plano | Riesgos

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

Acceso a una interfaz o sistema

- Uso de contraseñas débiles
- Mecanismos de recuperación de contraseñas inseguros
- Poca protección
- Falta de control de acceso

Impacto Técnico

- Pérdida o corrupción de información
- Denegación de servicio DDoS
- Compromiso dispositivo y/o cuentas de usuario

Impacto Negocio

- Económico
- Reputación

1. Uso de contraseñas débiles o en texto plano | Vulnerabilidades

¿Son mis contraseñas seguras?

- Determinar si la política de contraseña es suficiente en todas las interfaces a traves del uso de contraseñas débiles.
- 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.
- Nueva autenticación
- ¿Se permite la separación de roles en las interfaces?
- Revisar controles de acceso y escala de privilegios.

Ejemplo de ataque

Ataque por fuerza bruta → Contraseñas simples

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

Poca protección a través de la red (BASE64)

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

Contraseña encontrada:

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

1. Uso de contraseñas débiles o en texto plano | Mejores prácticas

¿Cómo asegurar el uso de contraseñas?

- 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
  - Control de acceso basado en roles (RBAC)

- Asegurar que las credenciales estén protegidas adecuadamente utilizando métodos de mejora de protección de contraseñas
  - Linux/Unix → shadow password

- Asegurar que los mecanismos de recuperación de contraseña sean seguros
  - Correo alternativo
  - Pregunta secreta

2. Uso de servicios de red inseguros | Riesgos

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

Comprometer un dispositivo	Impacto Técnico	Impacto Negocio
• Explotar vulnerabilidades • Usando debilidades del servicio de red • Capturar credenciales de inicio de sesión • Realizar ataques de buffer overflow y/o DDoS	• Pérdida de información sensible • Denegación de servicio DDoS • Apertura de ataques a otros dispositivos	• Interrupción de operaciones debido a DDoS.

2. Uso de servicios de red inseguros | Vulnerabilidades

¿Son mis servicios de red seguros?

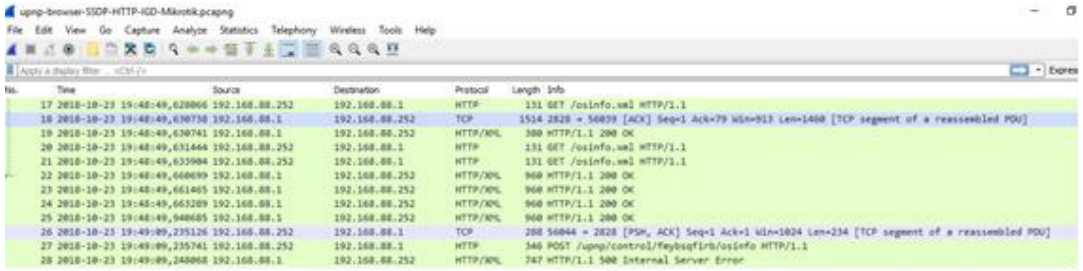
- Revisar el dispositivo en busca de puertos abiertos.
- Probar cada uno de los puertos abiertos en busca de vulnerabilidades (DDoS, servicios UDP, buffer overflow, fuzzing)
- Revisar los puertos de red para asegurarse de que sean absolutamente necesarios y si hay puertos expuestos a Internet mediante UpnP

Ejemplo de ataque

Ataque fuzzing → Deshabilitar el dispositivo

```
GET %s%s%s%s%s%s%s%s%s%s%s%s%s%s HTTP/1.0
```

Control del dispositivo (UpnP) → No hay autenticación



Permitiendo abrir puertos

```
Puertos 80 y 443 expuestos a Internet via
home router
```

2. Uso de servicios de red inseguros | Mejores prácticas

¿Qué hacer para que los servicios de red sean seguros?

- 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.

3. Uso de interfaces inseguras | Riesgos

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

Comprometer un dispositivo

- Uso de contraseñas débiles
- Falta de cifrado en el transporte
- Falta de autenticación
- Falta de bloqueo de cuentas

Impacto Técnico

- Pérdida o corrupción de información
- Denegación de servicio DDoS
- Compromiso total del dispositivo

Impacto Negocio

- Imagen
- Reputación

3. Uso de interfaces inseguras | Vulnerabilidades

¿Son mis interfaces seguras?

- 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.
- ¿Se permite 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 .
- Credenciales expuestas en redes inalámbricas.

Ejemplo de ataque interfaz web

Contraseña olvidada → Valida si una cuenta no existe

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

Restablecer contraseña → Validación existencia cuenta

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

Susceptible a XSS:

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

3. Uso de interfaces inseguras | Mejores Prácticas

¿Qué hacer para que la interfaz sea segura?

- 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

4. Falta de un mecanismo seguro de actualización de firmware | Riesgos

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

Acceso no autorizado

- Falta de sistema sencillo de actualización de dispositivo
- Falta de validación
- Falta de cifrado en el envío
- Falta de notificaciones

Impacto Técnico

- Pérdida o corrupción de información
- Denegación de servicio DDoS
- Compromiso dispositivo y/o cuentas de usuario

Impacto Negocio

- Económico
- Reputación

4. Falta de un mecanismo seguro de actualización de firmware | Vulnerabilidades

¿Es mi firmware seguro?

- Utilizar una herramienta de edición hexadecimal para revisar el archivo de actualización para 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, el servidor de actualización en la nube y el dispositivo.

Ejemplo de ataque

Archivo de actualización → HTTP

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

Archivo sin cifrado → legible para el ser humano

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

4. Falta de un mecanismo seguro de actualización de firmware | Mejores Prácticas

¿Cómo aseguro mi firmware?

- 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).

Requisitos críticos

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

5. Uso de librerías inseguras o desactualizadas | Riesgos

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

Compromiso del dispositivo

- Personalizaciones inseguras de plataforma de SO
- Uso de SW de terceras partes
- Uso de componentes HW comprometidos

Impacto Técnico

- Pérdida o corrupción de información
- Compromiso dispositivo y/o cuentas de usuario

Impacto Negocio

- Imagen
- Violación de privacidad

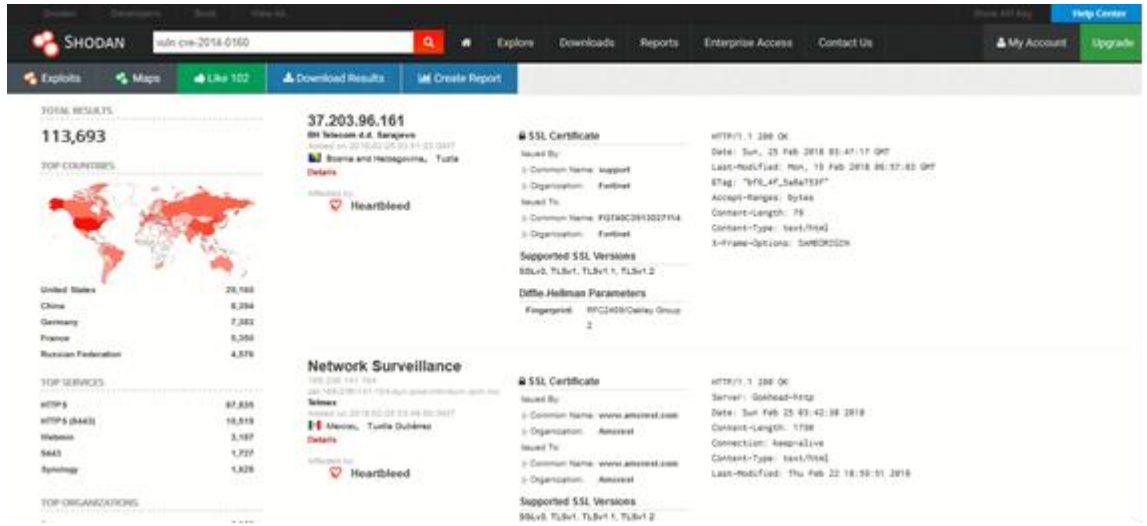
5. Uso de librerías inseguras o desactualizadas | Vulnerabilidades

¿Son mis componentes/librerías seguras?

- Conocer las versiones de todos los componentes que se utilizan.
- Revisar si el software es vulnerable, posee soporte o se encuentra desactualizado.
- 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.

Ejemplo de ataque

Vulnerabilidad Heartbleed de OpenSSL → CVE-2014-0160



5. Uso de librerías inseguras o desactualizadas | Mejores Prácticas

¿Qué hacer para evitar el uso de librerías o componentes obsoletos o desactualizados?

- 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

6. Insuficiente protección de la información personal o privada | Riesgos

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

Acceso al dispositivo

- Autenticación insuficiente
- Falta de cifrado en transporte
- Servicios de red inseguros
- Recolección innecesaria

Impacto Técnico

- Comprometer datos de usuarios
- Recopilación de datos personales

Impacto Negocio

- Violación de la privacidad
- Reputación
- Imagen
- Económico

6. Insuficiente protección de la información personal o privada | Vulnerabilidades

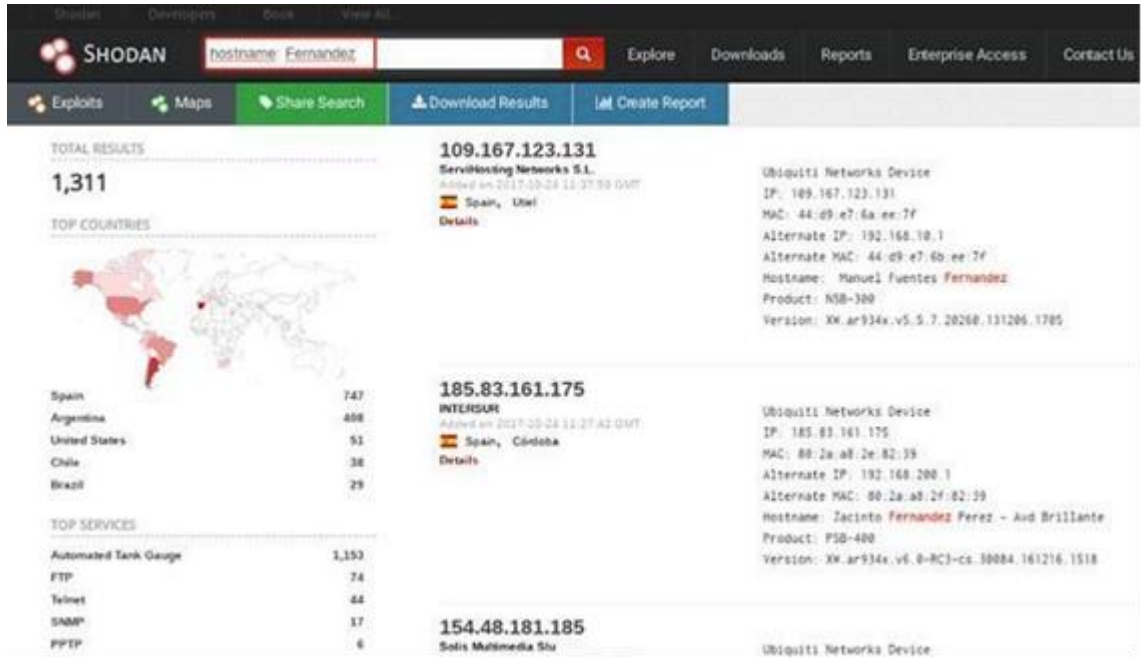
¿Esta protegida la información privada?

- 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.
- Cifrado correcto de la información 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 o si van más allá de la necesidad para el funcionamiento del dispositivo.
- Determinar si una política de retención de datos está en su lugar

Ejemplo de ataque

Exposición de información sensible o personal

```
Hostname: Fernández
```



6. Insuficiente protección de la información personal o privada | Mejores Prácticas

¿Qué hacer para proteger la información personal o privada?

- 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

7. Almacenamiento y transferencia de datos insegura | Riesgos

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

Acceso a la información

- Falta de cifrado
- Falta de control de acceso

Impacto Técnico

- Pérdida o corrupción de información
- Compromiso dispositivo y/o cuentas de usuario

Impacto Negocio

- Económico
- Imagen
- Violación de privacidad

7. Almacenamiento y transferencia de datos insegura | Vulnerabilidades

¿Uso cifrado para mis datos?

- 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

Ejemplo de ataque

Uso de HTTP

```
http://www.xyzcloudsite.com
```

Autenticacion de usuario y contraseña transmitida en texto plano

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

7. Almacenamiento y transferencia de datos insegura | Mejores Prácticas

¿Cómo proteger el almacenamiento y transferencia de datos?

- 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.

8. Falta de gestión de dispositivos | Riesgos

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

Acceso al dispositivo

- Mala configuración
- Poca protección
- Falta de permisos granulares
- Falta de cifrado
- Contraseñas débiles o inexistentes

Impacto Técnico

- Pérdida o corrupción de información
- Denegación de servicio DDoS
- Compromiso dispositivo

Impacto Negocio

- Reputación

8. Falta de gestión de dispositivos | Vulnerabilidades

¿Es mi gestión de dispositivos segura?

- Revisar la interfaz administrativa del dispositivo en busca de opciones para fortalecer la seguridad
- 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

Ejemplo de ataque

Tanto los administradores como usuarios tienen permisos para crear las contraseñas de sus cuentas.

No hay cifrado de datos → acceso a información sensible

8. Falta de gestión de dispositivos | Mejores Prácticas

¿Cómo gestionar los dispositivos de manera segura?

- 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

9. Uso de parámetros por defecto inseguros | Riesgos

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

Acceso no autorizado

- Mala configuración de seguridad
- Cuentas y/o configuraciones predeterminadas
- Servicios innecesarios
- Herencia

Impacto Técnico

- Pérdida o corrupción de información
- Pérdida de control del dispositivo

Impacto Negocio

- Reputación
- Imagen
- Económico

9. Uso de parámetros por defecto inseguros | Vulnerabilidades

¿Es mi configuración segura?

- Revisar el servicio a desplegar y buscar una configuración suficientemente fuerte.
- Revisar la reutilización de credenciales conocidas o el uso de contraseñas por defecto, débiles o muy conocidas.
- Revisar la instalación de características innecesarias.
- Revisar la configuración de los permisos.
- Revisar la existencia de cuentas predeterminadas con sus contraseñas activas y sin cambios.

Ejemplo de ataque

Acceso a cuentas de administrador por defecto

```
Username = admin; Password = 1234
```

Obtencion de credenciales por defecto

```
WWW-Authenticate: Basic realm="Default: admin/1234"
```

9. Uso de parámetros por defecto inseguros | Mejores Prácticas

¿Qué hago para mejorar la seguridad de mi configuración?

- 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”, “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

10. Falta de seguridad física en los dispositivos | Riesgos

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

Acceso al dispositivo

- Acceso al SO
- Acceso a información
- Puertos USB
- Puertos externos

Impacto Técnico

- Pérdida o corrupción de información
- Perdida de control de dispositivo

Impacto Negocio

- Reputación
- Imagen
- Económico

10. Falta de seguridad física en los dispositivos | Vulnerabilidades

¿Es mi seguridad física suficiente?

- 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 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 que el dispositivo cuenta con la espiral electromagnética
- Revisar que el dispositivo cuenta con un chip adicional dedicado exclusivamente al cifrado de la información almacenada

Ejemplo de ataque

Quitar la tarjeta SD e insertarla en un lector de tarjetas para ser alterada (modificada, copiada, etc.)

Acceder al software original del dispositivo a través de un puerto USB, para realizar modificaciones o copiar datos específicos.

10. Falta de seguridad física en los dispositivos | Mejores Prácticas

¿Cómo aseguro mis dispositivos físicos?

- 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).

CONCLUSIONES

1. Se han analizado los principales riesgos descritos por la OWASP.
2. Se han realizado diferentes pruebas para estudiar las vulnerabilidades asociadas a dichos riesgos.
3. Se han dado una serie de pautas o controles a seguir.

Se han cumplido con los objetivos del proyecto.

GRACIAS

Irene Salas Sanz