APUNTES 04

DETECCIÓN DE PROBLEMAS DE SEGURIDAD EN APLICACIONES PARA DISPOSITIVOS MÓVILES

PUESTA EN PRODUCCIÓN SEGURA

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

1. Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas.
2. Firma y verificación de aplicaciones.
3. Almacenamiento seguro de datos.
4. Validación de compras integradas en la aplicación.
5. Fuga de información en los ejecutables.
6. Soluciones CASB.

Caso práctico

Julián se ha embarcado en un nuevo proyecto para crear una app corporativa para los móviles de los empleados de una empresa. Está revisando aún las funcionalidades que requiere el cliente y pensando cómo y de qué manera podría abordarlas.

Uno de las preocupaciones que está en la cabeza de Julián es el gran número de requisitos que debe de cumplir su app para subirla a las principales tiendas de aplicaciones (Play Store, App Store, ...). Sabe que debe de acometer distintos procesos (reflejar permisos, firmar la app, etc) y que su aplicación tendrá que ser segura o podrían retirarla fácilmente de la tienda.

Por otra parte, la aplicación a desarrollar tiene que ser compatible con la tecnología de CASB que tiene el cliente, permitiendo el flujo de comunicación normal de la app y la comunicación con servicios externos.

Hoy en día debido a la cantidad de datos que posee sobre su dueño los teléfonos móviles se han convertido en el objetivo de los cibercriminales. Ya sea de forma directa o mediante apps maliciosas los atacantes buscan entrar a los datos contenidos en el dispositivo.

Durante los últimos meses varios programas (software o apps) maliciosos que controlan y espían el dispositivo móvil del usuario se han hecho famosos. Lo cierto es que, aunque pareciera no ser suficiente, los dispositivos cuentan con diversas protecciones ante este tipo de amenazas. Para ello el sistema operativo de los teléfonos móviles usan mecanismos para proteger la seguridad de los datos. Uno de los principales mecanismos de protección frente a apps maliciosas es el sandboxing, es decir, las aplicaciones corren en un entorno controlado y aislado para limitar el acceso y los permisos al sistema y a los datos.

1.- MODELOS DE PERMISOS EN PLATAFORMAS MÓVILES. LLAMADAS AL SISTEMA PROTEGIDAS.

Caso práctico

Julián sabe que para entender las vulnerabilidades de las aplicaciones móviles debe centrarse en los aspectos más importantes de seguridad de las mismas. Uno de estos aspectos son los modelos de permisos en las distintas plataformas móviles. Cada plataforma define un esquema de permisos, de manera que toda aplicación que acceda a determinados recursos está obligada a declarar su intención de usarlos. En caso de que una aplicación intente acceder a un recurso del que no ha solicitado permiso, se generará una excepción de permiso y la aplicación será interrumpida inmediatamente.

Tanto en iOS como en Android (principales sistemas operativos móviles) todas las aplicaciones se ejecutan en su propio sandbox o entorno aislado. En Android cada aplicación está funcionando con un usuario específico que se crea para esa aplicación mientras que en iOS todas las apps se ejecutan con el mismo usuario ("mobile") y cada aplicación tiene un directorio de inicio único para sus archivos, que se asigna aleatoriamente cuando se instala la aplicación.

Cuando una aplicación necesita acceder a partes de un sistema o a datos del usuario este tipo de acceso se considera protegido mediante permisos. Según cada plataforma funciona de manera distinta.

Cuando se instala una aplicación en Android que necesita acceder a alguna funcionalidad (fotos, cámara, contactos, etc) solicita al usuario permiso durante la instalación y el usuario verificará si es lícito o no. Existen dos niveles de acceso, accesos estándar o los más especiales o peligrosos. Una aplicación no podrá acceder a este tipo de funcionalidades o datos sin el consentimiento explícito del usuario. Las aplicaciones deben declarar antes de publicarse en la tienda oficial a que recursos necesitan tener acceso.

En iOS los permisos funcionan de manera algo distinta: las apps pueden acceder sólo a determinadas funciones que el sistema habilita, el resto no está permitido. Cuando una app necesita acceder a información del usuario usa un concepto de entitlement o permiso que está firmado digitalmente. Cuando una aplicación desea acceder a la cámara, fotos, ubicación o demás permisos, requiere que sea aprobado de forma explícita por el usuario de forma muy parecida a como sucede en Android.

Otro problema de seguridad adicional viene de la instalación de apps de terceros, fuera de la tienda oficial o bajadas de sitios web de dudosa reputación, si bien al final vuelven a necesitar que el usuario consiente el acceso (caso de Android) o no podrá acceder a menos de que tenga firmado ese acceso o el sistema lo permita (caso de iOS).

Para saber más; Existen numerosos tipos de permiso en el sistema Android, si quieres conocer en detalle cuales son y de qué manera se relacionan con la actividad del usuario puedes consultar más información en el siguiente enlace de la página para desarrolladores de Android.

2.- FIRMA Y VERIFICACIÓN DE APLICACIONES.

Caso práctico

Otro aspecto de la seguridad de las aplicaciones web, en la que debe centrarse Julián, es la firma y verificación de las aplicaciones. El proceso de firma y verificación de aplicaciones en aplicaciones móviles ayuda a garantizar que solo las aplicaciones auténticas y confiables, firmadas por desarrolladores verificados, puedan instalarse en los dispositivos.

Como comentábamos uno de los riesgos es el origen de las aplicaciones, es decir las tiendas o webs de aplicaciones de las plataformas móviles. Durante muchos años han sido un foco de Malware las tiendas no oficiales, los usuarios que descargan apps en webs de dudosa reputación e incluso aplicaciones poco recomendables disponibles en la tienda oficial.

Para solucionar estos problemas, actualmente todas las aplicaciones para móviles deben de pasar estrictos controles en la tienda oficial de apps. Uno de estos controles son las firmas digitales; las apps deben de estar firmadas por el desarrollador y si no lo están serán rechazadas por la tienda y además el instalador del dispositivo no permitirá instalarla.

Dentro de los controles establecidos por las tiendas oficiales para alojar una app, podríamos destacar:

- Una revisión exhaustiva de la la interacción que hacen con los datos de usuario.
- Los permisos que solicitan o requieren.
- Actualizaciones periódicas.
- Seguir y cumplir una serie de normas y políticas establecidas por la tienda oficial, etc.

Debes conocer: para saber algo más sobre los procesos de firma y verificación, puedes consultar en los siguientes enlaces las políticas de firma para desarrolladores de dos de las tiendas oficiales más populares: App Store (Apple) y Play Store (Google):

- Proceso de firma de código de apps en iOS y iPadOS Nueva ventana
- Proceso de firma de app en Google Nueva ventana

3.- ALMACENAMIENTO SEGURO DE DATOS.

Caso práctico

Aunque las aplicaciones hayan sido verificadas y el usuario haya consentido su uso y los permisos necesarios para que la app funcione, Julián sabe que un punto clave es el almacenamiento de datos dentro del dispositivo móvil. Este proceso es de vital importancia ya que habrá mucha información de carácter personal por lo que habrá que prestar atención a todo lo referente al nuevo Reglamento General de Protección de Datos (GDPR), que es el nuevo reglamento a nivel europeo para el tratamiento de datos personales.
Julián ha accedido a la versión en castellano del GDPR en este enlace Nueva ventana y cree que, prácticamente todo el mundo, debería tener conocimiento de los derechos y deberes que establece en cuanto a la privacidad y la protección de datos.

La mayoría de sistemas operativos móviles consiguen dotar de seguridad a este proceso mediante el cifrado de los datos almacenados. Uno de los métodos más comunes consiste en cifrar todo el sistema de ficheros (con sistemas de cifrado tanto simétrico como asimétricos) para que, si un usuario externo consigue acceso al dispositivo, no pueda leer su contenido. Cuando el usuario legítimo introduce su clave o accede mediante reconocimiento biométrico, esta información se usa como clave para descifrar el sistema de ficheros y que el usuario pueda interactuar con los datos sin problemas.
Keystore es la herramienta que proporciona Android para generar y almacenar de forma segura las claves usadas en los algoritmos de cifrado de la información, ya sea para la fase de cifrado como para la fase de descifrado.
Para iOS, existe la posibilidad de usar Keychain. En este caso, a diferencia de la estrategia provista en Android, podemos usar directamente Keychain para almacenar la información sensible del usuario que necesitemos, ya que la información que se almacena en Keychain será encriptada por el propio proceso que proporciona la API de Keychain. Sin embargo, también podemos usar Keychain de igual manera que se usa Keystore en Android, es decir, podemos usar Keychain para almacenar las claves que se usarán el proceso para cifrar y descifrar la información que almacenemos
Es de vital criticidad definir durante la fase de diseño de la aplicación una robusta y correcta estrategia para el almacenado de los datos sensibles del usuario, si queremos que nuestra aplicación cumpla con los requisitos de seguridad exigidos en nuestros días.
Debes conocer: El objetivo principal de securizar los datos del dispositivo móvil es prevenir la fuga de información del dispositivo.

4.- VALIDACIÓN DE COMPRAS INTEGRADAS EN LA APLICACIÓN.

Caso práctico

Uno de los aspectos en los que las plataformas de móviles ponen más énfasis es en prevenir el pago no autorizado de dinero a través de aplicaciones y sin el conocimiento del usuario del dispositivo. Teniendo en cuenta que ahora mismo no solamente es posible pagar a través del teléfono móvil sino que incluso podemos pagar desde los relojes inteligentes (smartwatches) Julián entiende que todo tiene que estar controlado y el usuario ser consciente.

La validación de compras integradas se vuelve esencial para prevenir fraudes, garantizar la autenticidad de las transacciones y proteger la información financiera de los usuarios. Los desafíos incluyen la falsificación de compras, el robo de identidad y la manipulación de datos de transacciones.
El proceso de compras a través de las aplicaciones sigue determinados mecanismos de protección, desde canales seguros de comunicaciones para prevenir ataques de Man-In-The-Middle cómo procesos de autenticación y validación expresa por parte del usuario.
Veamos algunos de estos mecanismos:

1. **Criptografía y Firma Digital:**

Implementar algoritmos de criptografía robustos y firmas digitales ayuda a asegurar la integridad de los datos de compra. Esto impide la manipulación de la información durante la transmisión, garantizando que solo las transacciones legítimas sean aceptadas.

2. **Autenticación Multifactor (AMF):**

La AMF añade una capa adicional de seguridad, exigiendo la verificación de la identidad del usuario mediante múltiples métodos, como contraseñas, códigos de un solo uso o biometría. Esto dificulta la usurpación de cuentas y fortalece la autenticación.

3. **Monitoreo de Patrones Anómalos:**

La implementación de sistemas de monitoreo en tiempo real permite la detección temprana de patrones de actividad inusuales o transacciones sospechosas. Esto posibilita respuestas rápidas ante posibles amenazas y minimiza el impacto de posibles incidentes de seguridad.

Además, hay que fomentar la conciencia entre los usuarios sobre las mejores prácticas de seguridad, como la importancia de proteger las credenciales de la cuenta y la necesidad de mantener sus dispositivos actualizados, contribuye significativamente a la prevención de ataques.
Debes conocer: Seguro que encuentras interesante este enlace Nueva ventana de métodos de pago y su seguridad del blog de INCIBE

5.- FUGA DE INFORMACIÓN EN LOS EJECUTABLES.

Caso práctico

Julián sabe que los ejecutables de las aplicaciones móviles pueden ser analizados y manipulados. Este riesgo puede ser explotado por ciberdelicuentes con el objetivo de obtener información sensible, eludir medidas de seguridad, introducir malware o incluso realizar ataques de falsificación de identidad.

La ingeniería inversa de una aplicación móvil es el proceso de analizar la aplicación compilada para extraer información sobre su código fuente. Este proceso implica analizar el código binario (análisis estático del código) o la ejecución (análisis dinámico) de una aplicación con el objetivo de comprender su estructura interna y lógica de funcionamiento. Si bien este enfoque puede ser legítimo, como parte del análisis de seguridad por parte de los desarrolladores, también abre la puerta a posibles actividades maliciosas.

Los ciberdelincuentes aprovechan la ingeniería inversa para descubrir información sensible de la aplicación, vulnerabilidades de seguridad y algoritmos críticos. Esta práctica, a menudo facilitada por herramientas de compilación, permite la extracción no autorizada de información sensible, incluyendo claves de autenticación y datos críticos del usuario.

Además, existe la posibilidad del Tampering, o manipulación no autorizada de aplicaciones móviles, lo que implica alterar el código binario o su entorno para afectar a su comportamiento. Este riesgo puede ser explotado por ciberdelicuentes con el objetivo de eludir medidas de seguridad, introducir malware o incluso realizar ataques de falsificación de identidad.

Para mitigar estos riesgos, los desarrolladores y profesionales de ciberseguridad adoptan medidas defensivas, como la ofuscación de código, el cifrado robusto y la implementación de técnicas de detección de manipulación. Estas estrategias buscan no solo proteger la propiedad intelectual y la información confidencial, sino también preservar la integridad y la autenticidad de las aplicaciones móviles.

Para saber más: OWASP tiene un proyecto para las pruebas de seguridad de aplicaciones móviles (MASTG), mira este enlace Nueva ventana si quieres saber más sobre Ingeniería Inversa y Tampering y este otro enlace Nueva ventana para ver algunas técnicas disponibles

6.- SOLUCIONES CASB.

Caso práctico

Julián sabe que muchas veces el dato no solamente está en el dispositivo sino también almacenado en servicios o aplicaciones que utilizan los entornos de nube o cloud . Los problemas que surgen en estos casos son varios, desde el poco control a no tener reglas de detección y bloqueo.

Además, y unido a situaciones como el teletrabajo, muchos usuarios hacen uso de sus dispositivos móviles personales para acceder a servicios en nube corporativos o de terceros perdiéndose la trazabilidad y control de la información. Estos servicios en nube incluyen desde correo hasta imágenes o ficheros.

Es aquí donde entra la tecnología de CASB.

Este tipo de tecnología viene a dar solución a estos problemas, aportando visibilidad sobre la información, monitorización y trazabilidad. Con esto podremos saber qué flujo sigue un determinado documento o qué tipo de información esta saliendo o entrando en un dispositivo móvil.

Hoy en día la tecnología de CASB se está extendiendo rápidamente por las empresas, ya que se han dado cuenta que no solamente es importante securizar tu entorno, servidores y demás, sino también los entornos de nube pero, sobre todo, los dispositivos móviles.

A nivel técnico funciona como un agente que se instala en el dispositivo y que recibe de forma centralizada la lista de políticas y reglas establecidas. De manera que, por un lado, se puede detectar que esta haciendo el dispositivo y, además, limitar el acceso a los servicios de nube o prevenir que se suba o baje determinada información de los mismos. Algunas soluciones de CASB avanzada disponen de capacidad UEBA que permite analizar patrones de comportamiento de los usuarios.

Finalmente la mayoría de soluciones consiguen cifrar los datos antes de enviarlos a la nube, lo que supone un control más y una capa de seguridad adicional para prevenir la fuga de información.

Para saber más: Si deseas conocer más sobre las soluciones de CASB, tanto a nivel de capacidades tecnológicas como de modelo operativo y algunos de los principales fabricantes de referencia de este tipo de tecnología puedes hacerlo en este enlace Nueva ventana

Respuestas

Autoevaluación I: 1 b), 2b), 3 a), 4 a)

Autoevaluación II: 1 a), 2b), 3 b), 4 b)

TEST I 10/10: 1 b), 2 a), 3 d), 4 a), 5 c), 6 c), 7 b), 8 a), 9 a), 10 a)

TEST II 9/10: 1 a), 2 b), 3 a), 4 b), 5 a), 6 a), 7 a), 8 a), 9 a), 10 a)

Autoevaluación I

Identifica si las siguientes frases son verdaderas o falsas

1- Una aplicación puede acceder a los datos del dispositivo móvil sin autorización previa
   a) Verdadero
   b) Falso

2- Cualquiera puede subir una aplicación a una de las tiendas oficiales sin apenas control.
   a) Verdadero
   b) Falso

3- Los dispositivos móviles se han convertido en un objetivo de los cibercriminales.
   a) Verdadero
   b) Falso

4- Durante los últimos meses han surgido software malicioso para móviles que es capaz de monitorizar y espiar la actividad y datos de los usuarios.
   a) Verdadero
   b) Falso

Autoevaluación II

1- Las soluciones de CASB aportan una capa mas de detección de fuga de información
   a) Verdadero
   b) Falso

2- Los sistemas operativos móviles y las apps no suelen implementar controles para las compras integradas.
   a) Verdadero
   b) Falso

3- Los empleados de una compañía suelen usar para acceder a los datos tanto terminales corporativos como los suyos propios personales.
   a) Verdadero
   b) Falso

4- Los sistemas de CASB es la solución definitiva para la fuga de información en entornos de nube.
   a) Verdadero
   b) Falso

TEST I

1- No hay regulaciones especiales para el tratamiento de datos de caracter personal. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

2- Los permisos especiales de iOS están firmados digitalmente. ¿Verdadero o Falso?
   a) Verdadero
   b) Falso

3- ¿Qué significa CASB?:
   a) Cloud Advance Security Broker.
   b) Created Advanced Security Bureau.
   c) Cloud Advanced Security Brokers.
   d) Cloud Access Security Brokers.

4- Las apps subidas a las tiendas oficiales deben de cumplir bastantes requisitos. ¿Verdadero o Falso?
   a) Verdadero
   b) Falso

5- Que es GDPR:
   a) Estandard de comunicación de los dispositivos móviles.
   b) Tipo de protocolo.
   c) Reglamento General de Protección de Datos.
   d) Función especial de iOS.

6- ¿Cómo gestionan las claves las plataformas móviles?:
   a. Sistemas de nube.
   b. Mediante CASB.
   c. Mediante sistemas de gestión de claves.
   d. En memoria.

7- ¿Qué llave se usa en algunos sistemas operativos de móviles para cifrar?:
   a. La llave se genera en tiempo real.
   b. código desbloqueo o datos biométricos.
   c. nombre de usuario.
   d. fecha de nacimiento usuario.

8- Los teléfonos móviles se han convertido en el objetivo de los cibercriminales. ¿Verdadero o Falso?
   a) Verdadero
   b) Falso

9- Los permisos especiales de iOS están firmados digitalmente. ¿Verdadero o Falso?
   a) Verdadero
   b) Falso

10- El dispositivo móvil contiene mucha información de caracter personal. ¿Verdadero o Falso?
   a) Verdadero
   b) Falso

TEST II

1- CASB aporta visibilidad sobre entornos de nube. ¿Verdadero o Falso?
   a) Verdadero
   b) Falso

2- Cual de las siguientes se considera una forma de limitar las capacidades de una aplicación en un dispositivo móvil:
   a. Chrooting.
   b. Permisos.
   c. Jailbreak.
   d. Conectividad.

3- ¿Qué factor ha impulsado la tecnología CASB?:
   a. Teletrabajo.
   b. Machine learning.
   c. Número de vulnerabilidades.
   d. Transformación tecnológica.

4- No supone un problema que los empleados usen sus teléfonos personales para tareas corporativas. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

5- ¿Cuando una aplicación solicita permisos?:
   a. Durante la instalación y ejecución.
   b. Durante la instalación
   c. Durante la ejecución.
   d. Durante la descarga.

6- Los sistems de CASB tienen el objetivo de aportar visibilidad. ¿Verdadero o Falso?
   a) Verdadero
   b) Falso

7- Los sistemas de CASB tienen el objetivo de aportar visibilidad. ¿Verdadero o Falso?
   a) Verdadero
   b) Falso

8- Las apps de iOS requieren permisos al usuario en la instalación?:
   a. No, solamente algunas funcionales especiales de privacidad pueden solicitar permiso del usuario.
   b. Si, siempre.
   c. Si, según la versión del sistema operativo.
   d. Según se configure la app por el desarrollador.

9- Las aplicaciones piden autorización expresa para realizar compras. ¿Verdadero o Falso?
   a) Verdadero
   b) Falso

10- Las apps de iOS tienen un directorio único donde se ejecutan e instalan sus ficheros. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

Caso práctico

Julián ha estado trabajando en un proyecto de una aplicación móvil junto con una solución CASB que quiere salir al mercado y ser revolucionaria.

Para comprobar que la aplicación es segura se ha seguido la última versión de la Guía de Pruebas de Seguridad de Aplicaciones Móviles (MASTG) desarrollada por OWASP. Julián entiende que el Estándar de Verificación de Seguridad de Aplicaciones Móviles (MASVS) proporciona un marco claro y detallado que aborda los requisitos de seguridad esenciales para el desarrollo y la evaluación de aplicaciones móviles. Por otro lado, la Guía de Pruebas de Seguridad de Aplicaciones Móviles (MASTG) se alinea estrechamente con los requisitos establecidos por la MASVS, ofreciendo un conjunto adicional de directrices específicas para realizar pruebas de seguridad efectivas en aplicaciones móviles. La combinación de ambas herramientas, MASVS y MASTG, proporciona un enfoque integral para evaluar y mejorar la seguridad en aplicaciones móviles, permitiendo a los profesionales adaptar sus estrategias según el contexto específico.

Uno de los puntos que más se han trabajado durante el proyecto de la solución CASB es ser diferenciadores y poder corregir los problemas de adopción que han tenido las soluciones de MDM (Mobile Device Management). Saben que las soluciones para móviles tienen que ser capaces de lidiar con varios problemas como la privacidad, BYOD (Bring Your Own Device), etc.

Esta tarea es eminentemente teórica donde el alumno deberá responder y desarrollar una serie de preguntas. El alumno debe saber manejar guías para comprobar si una aplicación móvil es segura o no, entender distintos conceptos como CASB, MDM, BYOD, etc y ser capaz de entender que capacidades aportan las soluciones tecnológicas, con qué problemas se encuentran en el mercado y qué capacidades adicionales podrían tener y qué las empresas valorarán.

Apartado 1: MASTG

En la unidad 2 ya vimos que OWASP ha desarrollado el proyecto Mobile Application Security (MAS) que proporciona un estándar de seguridad para aplicaciones móviles (OWASP MASVS) y una guía de pruebas exhaustiva (OWASP MASTG) que cubre los procesos, técnicas y herramientas utilizados durante una prueba de seguridad de aplicaciones móviles, así como un conjunto exhaustivo de casos de prueba que permite a los probadores ofrecer resultados coherentes y completos.
En este apartado se pide revisar la guía MASTG, centrándose en las diferentes defensas contra la Ingeniería Inversa en Android (Android Anti-Reversing Defenses) y en IOS (IOS Anti-Reversing Defenses).

1- Una medida defensiva es comprobar el "Rooteado" en Android y el "Jailbreak" en IOS. Rellena la siguiente tabla utilizando la guía MASTG.

¿Qué son los dispositivos rooteados o con jailbreak?	Son dispositivos a los que se les han eliminado las restricciones del fabricante. Esto permite al usuario tener un control total sobre el sistema operativo, pudiendo instalar aplicaciones no oficiales, personalizar el dispositivo y acceder a funciones avanzadas. Sin embargo, aumenta los riesgos de seguridad.
Indica 1 medida para comprobar el rooteado	Para comprobar que un dispositivo Android está rooteado se puede utilizar la aplicación Root Checker. Verifica si el dispositivo tiene acceso al superusuario (root) y proporciona un informe sobre su estado.
Indica 1 medida para comprobar el Jailbreak	Para comprobar que un dispositivo iOS tiene jailbreak, se puede buscar la aplicación Cydia en el dispositivo. Es una tienda de aplicaciones alternativas que solo estarán disponibles para ese tipo de dispositivos.

2- Otra medida defensiva es la ofuscación. Rellena la siguiente tabla utilizando la guía MASTG.

¿ En qué consiste la ofuscación?	Técnica de seguridad que transforma el código legible, en algo difícil de leer (formato ininteligible) y entender para los humanos, pero que sigue funcionando igual. Se hace para proteger el código de los atacantes que intentan analizarlo o modificarlo. (ejemplo: cambiar nombres de funciones)
Indica para qué se utiliza la herramienta ProGuard y cómo se utiliza	Herramienta de línea de comandos que se usa en aplicaciones Android para reducir, optimizar y ofuscar el código (Java). Ayuda a hacer el archivo APK más pequeño y seguro. Para utilizarlo se añade una configuración en el archivo build.grandle, activando la opción minifyEnabled y especificando las reglas de la herramienta.
Indica para qué se utiliza la herramienta SwiftShield y cómo se utiliza	Es una herramienta para aplicaciones iOS que ofusca el código escrito en Swift. Protege la lógica y la propiedad intelectual de la aplicación contra la ingeniería inmersiva. Para usarlo, se integra en el proceso de compilación del proyecto, configurando las opciones de ofuscación en el archivo de configuración del proyecto.

3- Explorar aplicaciones utilizando un depurador es una técnica muy poderosa. No solo se puede rastrear variables que contienen datos confidenciales y modificar el flujo de control de la aplicación, sino también leer y modificar la memoria y los registros. Rellena la siguiente tabla utilizando la guía MASTG.

Explica qué consiste la técnica antidepuración JDWP en Android	(Java Debug Wire Protocol) Se utiliza para evitar que los atacantes depuren la aplicación. Es un protocolo que permite la depuración de aplicaciones Java y en Android se usa para depurar aplicaciones en ejecución. Para proteger la aplicación, se puede implementar medidas que detecten si un depurador está conectado y si es así, cerrar la aplicación o cambiar su comportamiento para dificultar la depuración.
Explica qué es ptrace y cómo se puede utilizar para evitar la depuración en IOS	Es una función en sistemas Unix que permite controlar un proceso a través de otro (proceso padre), lo que es útil para la depuración. En iOS, se puede usar esta herramienta con la opción PT_DENY_ATTACH para evitar que otros depuradores se adjunten a la aplicación. Si un depurador intenta adjuntarse, el proceso se termina automáticamente (porque el proceso padre observa, examina y controla el resto de procesos), lo que dificulta la depuración por parte de los atacantes.

4- La presencia de herramientas, frameworks y aplicaciones comúnmente utilizadas por la ingeniería inversa puede indicar un intento de realizar ingeniería inversa en la aplicación. Algunas de estas herramientas sólo pueden ejecutarse en un dispositivo con jailbreak o rooteado, mientras que otras obligan a la aplicación a entrar en modo de depuración o dependen del inicio de un servicio en segundo plano en el teléfono móvil. Por lo tanto, existen diferentes formas que una aplicación puede implementar para detectar un ataque de ingeniería inversa y reaccionar ante él, por ejemplo, finalizándose ella misma. Utilizando la guía MASTG.

Explica qué es y para que se utiliza la herramienta Frida	Es una herramienta de instrumentación dinámica que permite a los desarrolladores y analistas de seguridad inyectar código en aplicaciones móviles a tiempo real. Esto significa que pueden observar y modificar el comportamiento de una aplicación mientras se ejecuta. Se utiliza para el análisis de seguridad, la depuración y la ingeniería inversa de aplicaciones en múltiples plataformas (incluyendo Android e iOS)
Explica cómo se puede detectar en IOS (Frida Detection)	Para detectar si una aplicación está siendo manipulada con Frida en iOS, se pueden implementar diferentes técnicas. Una de ellas es buscar la presencia de procesos o librerías asociadas con Frida (frida-server o FridGadget.dylib). Otra técnica, es monitorear las conexiones de red inusuales que podrían indicar que Frida está interactuando con la aplicación.

Apartado 2: MDM y CASB

Los servicios CASB (Cloud Access Security Broker) y las plataformas MDM (Mobile Device Management) desempeñan roles esenciales en la seguridad de la información en entornos empresariales modernos. La combinación de CASB y MDM proporciona un enfoque integral para abordar las amenazas modernas, asegurando tanto los datos en la nube como los dispositivos móviles, lo que es crucial para salvaguardar la integridad y confidencialidad de la información empresarial.

1- Rellena la siguiente tabla comparativa CASB vs MDM

	CASB	**MDM**
Objetivo principal	(Cloud Access Security Broker) Proteger y controlar el acceso a los datos y aplicaciones en la nube. Actúa como un intermediario entre los usuarios y los servicios en la nube para asegurar el cumplimiento de las políticas de seguridad.	(Mobile Device Management) Gestionar y asegurar los dispositivos móviles utilizados en una organización (smartphones, tablets y otros dispositivos). Garantizando que cumplan con las políticas de seguridad de la empresa.
Alcance y enfoque	Seguridad de aplicaciones y datos en la nube, proporcionando visibilidad, control y protección contra amenazas para todas las aplicaciones (autorizadas como no autorizadas).	Gestión y seguridad de dispositivos móviles, controlando el acceso a recursos, administrando aplicaciones y configuraciones y protegiendo los datos almacenados en el dispositivo.
Gestión (¿qué elementos se gestionan?)	Acceso a aplicaciones y datos en la nube, monitoreo del uso de las aplicaciones, prevención de pérdida de datos y detección de amenazas.	Dispositivos móviles, incluyendo instalación de aplicaciones, configuración de políticas de seguridad, monitoreo de dispositivos, protección de datos (mediante cifrado) y eliminación remota, por pérdida o robo.
Arquitectura (¿cómo se implementa?)	Generalmente se implementa como un servicio en la nube, que actúa como intermediario entre los usuarios y las aplicaciones en la nube. Pueden funcionar como un proxy directo o inverso.	Se implementa a través de un servidor central que gestiona los dispositivos móviles conectados. Puede ser una solución basada en la nube o en las instalaciones de la empresa.
¿Qué problemas o limitaciones tiene cada una (por ejemplo, con la protección de datos)?	Pueden ser complejos de configurar y gestionar, y pueden no cubrir todas las aplicaciones SaaS utilizadas por la empresa. También pueden tener limitaciones en la integración con soluciones de identidad y acceso.	Pueden ser difíciles de implementar y gestionar debido a la diversidad de dispositivos y sistemas operativos. Además, pueden enfrentar problemas de compatibilidad y fragmentación (especialmente en dispositivos Android)
Da 3 ejemplos de soluciones MDM y 3 CASB	Netskope Microsoft Cloud App Security. McAfee Mvision Cloud	AirDrod Business Scalefusion Hexnode

A la hora de escoger una solución CASB es importante conocer cuales son las características más importantes de las mismas.

2- Rellena la siguiente tabla, identificando y describiendo detalladamente y con un ejemplo al menos cinco características clave que suelen ofrecer las soluciones CASB (ejemplo: control de acceso, prevención de fuga de datos, etc.). Como ejemplo de lo que se pide se rellena una característica típica como el control de acceso.

Característica	Descripción detallada	Ejemplo
Control de acceso y autenticación	Implementa políticas de acceso basadas en el contexto, como ubicación, tipo de dispositivo, nivel de riesgo o autenticación multifactor (MFA). Se puede restringir el acceso en función del usuario o del rol dentro de la empresa.	Un usuario intenta acceder a la aplicación de contabilidad desde un dispositivo no administrado. El CASB impide el acceso o solicita autenticación adicional.
Prevención de pérdida de datos (DLP)	Protege la información confidencial evitando que se compartan o se transmitan de manera no autorizada. Utiliza políticas para identificar y bloquear la transmisión de datos sensibles, como números de tarjetas de crédito o información personal	Un empleado intenta enviar un correo electrónico con un archivo que contiene datos de clientes. El CASB detecta la información sensible y bloquea el envío del correo.
Visibilidad y monitoreo	Proporciona una visión completa del uso de aplicaciones en la nube, incluyendo quién accede, qué datos se comparten y cómo se utilizan las aplicaciones. Esto ayuda a identificar comportamientos sospechosos y a tomar medidas preventivas.	El equipo de seguridad puede ver que un usuario está descargando grandes cantidades de datos desde una aplicación en la nube fuera de horario laboral, podría indicar una actividad no autorizada.
Protección contra amenazas	Detecta y responde a comportamientos anómalos y amenazas en la nube, como malware, ransomware o accesos no autorizados. Utiliza un análisis avanzado para identificar y mitigar riesgos en tiempo real.	El CASB detecta el intento de acceso desde una ubicación geográfica inusual y bloquea el acceso para evitar una posible brecha de seguridad.
Cumplimiento normativo	Ayuda a la empresa a cumplir con las regulaciones y normativas de seguridad, como GDPR, HIPAA o PCI- DSS. Proporciona herramientas para auditar y reportar el cumplimiento de políticas de seguridad en la nube.	Una empresa necesita demostrar que cumple con las regulaciones de protección de datos. El CASB genera informes detallados sobre el uso de datos y las medidas de seguridad implementadas.
Evaluación y administrador	Identifica y gestiona el uso de aplicaciones en la nube no autorizadas por la empresa, conocidas como Shadow IT. Esto ayuda a controlar los riesgos asociados con el uso de aplicaciones no aprobadas.	El CASB detecta que varios empleados están utilizando una aplicación de almacenamiento en la nube no autorizada y bloquea su uso para proteger los datos corporativos.

Apartado 3: Diseño y capacidades de CASB

Elige una solución CASB disponible en el mercado (ejemplo: Microsoft Defender for Cloud Apps, Netskope, McAfee MVISION Cloud, Palo Alto Prisma Access,etc.).

1- Rellena la siguiente tabla describiendo cinco características de dicha solución que te han parecido las más importantes (deben ser distintas a las que has puesto en el apartado 2.2). Justifica por qué te parecen importantes.

Característica	Justificación
Análisis de comportamiento de usuarios y entidades (UEBA)	Esta característica utiliza inteligencia artificial para analizar el comportamiento de los usuarios y detectar actividades inusuales que podrían indicar una amenaza. Es importante porque ayuda a identificar y mitigar riesgos antes de que se conviertan en problemas graves.
Control de aplicaciones no autorizadas (Shadow IT)	Permite a las empresas identificar y gestionar el uso de aplicaciones en la nube que no han sido aprobadas oficialmente. Esto es crucial para evitar riesgos de seguridad asociados con el uso de aplicaciones no controladas.
Protección de datos a tiempo real	Y monitorea y protege los datos en tiempo real mientras se mueven entre dispositivos y aplicaciones en la nube. Esto es esencial para prevenir la pérdida de datos y garantizar que la información sensible esté siempre segura.

Integración con otras soluciones de seguridad	Se integra fácilmente con otras herramientas de seguridad, como soluciones de gestión de identidades y accesos y sistemas de información y gestión de eventos de seguridad. Esta integración mejora la capacidad de respuesta ante incidentes y proporciona una visión más completa de la seguridad.
Cumplimiento normativo automatizado	Ayuda a las empresas a cumplir con regulaciones normativas de seguridad mediante la ayuda automatización de políticas y generación de informes de cumplimiento. Esto es importante para reducir el riesgo de sanciones y mantener la confianza en los clientes.
Cifrado de datos	Esta característica asegura que los datos sensibles estén cifrados tanto en tránsito como en reposo. El cifrado protege la información contra accesos no autorizados, incluso si los datos son interceptados o robados. Es crucial mantener la confidencialidad y la integridad de los datos empresariales.
Gestión de entidades y accesos (IAM)	Integra capacidades avanzadas de gestión de identidades y accesos, permitiendo una administración centralizada de las identidades de los usuarios y sus permisos. Esto es importante para garantizar que solo las personas autorizadas puedan acceder a los datos y aplicaciones sensibles, reduciendo el riesgo de accesos no autorizados

2- Responde a las siguientes cuestiones:

¿Qué problema supone cuando un usuario se va de la empresa en un entorno de BYOD (Bring Your Own Device)?

Cuando un usuario abandona la empresa en un entorno BYOD surgen diferentes problemas de seguridad y gestión:

- Un antiguo trabajador puede seguir teniendo acceso a datos y aplicaciones corporativas desde su dispositivo personal, lo que representa un riesgo significativo de fuga de información confidencial.
- La empresa pierde la capacidad de gestionar y controlar el dispositivo, lo que dificulta la implementación de políticas de seguridad y la protección de datos sensibles de la organización.
- Existe el riesgo de que el usuario utilice el dispositivo con un fin malintencionado, existe la posibilidad de que el antiguo trabajador utilice la información y los accesos para fines maliciosos, como compartir datos con personas externas (competencia) o realizar actividades fraudulentas.
- Quitar los accesos a aplicaciones y datos corporativos en dispositivos personales puede ser complicado y no siempre puede resultar efectivo, especialmente si el dispositivo no está bajo la gestión de la empresa.

¿Qué mecanismos deberías tener en la solución CASB que has plateando en el apartado 3.1 para cuando un usuario abandone la compañía y siga siendo compatible con BYOD?

Para abordar dichos problemas, la solución CASB (Microsoft Defender for Cloud Apps) debe incluir los siguientes mecanismos:

- El CASB debe permitir la revocación inmediata de accesos a aplicaciones y datos corporativos en cuanto se detecte que un usuario ha dejado la empresa. Se podría realizar mediante la integración con sistemas de gestión de identidades y accesos (IAM) para desactivar cuentas y permisos de forma centralizada.
- Implementar alguna política que restrinja el acceso a datos sensibles desde dispositivos no administradores o no autorizados. Esto asegura que, una vez que el usuario deja la empresa, su dispositivos personal no pueda acceder a los datos, no podrá leerlos sin las claves de acceso adecuadas.
- Mantener un monitoreo o auditoría constante de las actividades de los usuarios y generar alertas en caso de comportamientos sospechosos. Esta ayuda a detectar y responder rápidamente a cualquier intento de acceso no autorizado después de que un usuario se haya ido de la empresa.
- Implementar políticas de DLP (Prevención de Pérdida de datos) que bloqueen la transferencia de datos sensibles a dispositivos no autorizados o a ubicaciones no seguras. Esto previene que los ex-empleados puedan copiar o transferir información crítica fuera de la red corporativa.
- Integrar la solución CASB con sistemas de gestión de dispositivos móviles (MDM) para asegurar la eliminación remota de datos corporativos en caso de necesidad.

Cuando un empleado deja la empresa en un entorno BYOD, puede seguir teniendo acceso a datos sensibles, lo que representa un riesgo de seguridad. Para mitigar estos riesgos, es esencial usar una solución CASB como Microsoft Defender Cloud Apps, que permite revocar accesos en tiempo real, controlar dispositivos no autorizados, cifrar datos, monitorear actividades y cumplir con normativas de seguridad. Estos mecanismos aseguran que la información corporativa permanezca protegida bajo control, incluso cuando se utilizan dispositivos personales.