

Detección de problemas de seguridad en aplicaciones para dispositivos móviles.

Caso práctico

Julián ha terminado de trabajar en el proyecto del aplicativo web y ahora 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.



[Torsten Dettlaff](#) (Licencia de Pexels)

Uno de las preocupaciones que está en la cabeza de Julián es el gran número de requisitos que debe de cumplir su app para subir a las principales tiendas de aplicaciones. 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 software 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.



[Ministerio de Educación y Formación Profesional](#) (Dominio público)

Materiales formativos de FP Online propiedad del Ministerio de Educación y Formación Profesional.

[Aviso Legal](#) 

1.- Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas.

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.



[Pexels](#) (Dominio público)


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 de aplicaciones a que recursos necesitan accesos.

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 permiso 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 fuera de la tienda oficial o bajadas de sitios web de dudosa reputación, si bien al final vuelven a necesitar que el usuario consienta 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 cuáles 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.

Como comentábamos uno de los riesgos es el origen de las aplicaciones, es decir la tienda oficial de aplicaciones de la plataforma móvil. Durante muchos años ha sido un foco de Malware tiendas no oficiales, usuario bajando apps en webs de dudosa reputación e incluso aplicaciones poco recomendables disponibles en la tienda oficial.



[Pexels](#) (Dominio público)

Para solucionar estos problemas 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 de la tienda y además el instalador del dispositivo no permitirá instalarla.

Dentro de los controles a los que someten las apps las tiendas oficiales, tendríamos una revisión exhaustiva de la interacción que hacen con los datos de usuario, los permisos que necesitan, estar actualizadas, seguir una serie de normas y políticas, etc.

Autoevaluación

Identifica si las siguientes frases son verdaderas o falsas

Una aplicación puede acceder a los datos del dispositivo móvil sin autorización previa

☐ Verdadero ☐ Falso

Falso

Todo acceso a datos del tanto del usuario como funcionalidades debe hacerse a través de permisos.

Cualquiera puede subir una aplicación a una de las tiendas oficiales sin apenas control.

☐ Verdadero ☐ Falso

Falso

Las aplicaciones que se suben a la tienda oficial pasan distintos controles de seguridad para garantizar su seguridad y la de los usuarios.

Los dispositivos móviles se han convertido en un objetivo de los cibercriminales.

☐ Verdadero ☐ Falso

Verdadero

Contienen gran cantidad de información y de mucho valor.

Durante los últimos meses han surgido software malicioso para móviles que es capaz de monitorizar y espiar la actividad y datos de los usuarios.

☒ Verdadero ☐ Falso

Verdadero

Un ejemplo sería el software Pegasus.

3.- Almacenamiento seguro de datos.

Aunque las aplicaciones hayan sido verificadas y el usuario haya consentido su uso y los permisos necesarios para que la app funcione, llega el momento clave que 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.



[Pexels](#) (Dominio público)

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 dactilar o fácil 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 necesitamos, 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

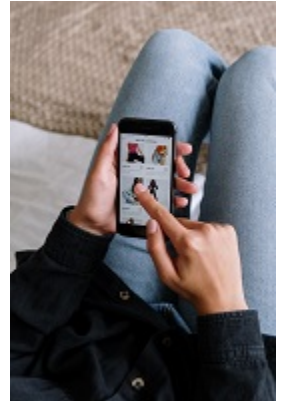
El objetivo principal de securizar los datos del dispositivo móvil es prevenir la fuga de información del dispositivo.

4.- Validación de compras integradas en la aplicación.

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*) todo tiene que estar controlado y el usuario ser consciente.

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.



[Pexels](#) (Dominio público)

Debes conocer

Seguro que encuentras interesante este [link](#)  de discusión sobre el uso de MD5.

5.- Soluciones CASB.

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.



[Pexels](#) (Dominio público)

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

Hoy en día la tecnología de CASB se está extendiendo rápida por las empresas, ya que se han dado cuenta que no solamente es importante secularizar 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 establecida. De manera que por un lado se puede detectar que esta haciendo el dispositivo como 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 (User and Entity Behaviour Analytics) que permite analizar patrones de comportamiento de los usuarios.

Finalmente la mayoría de soluciones consiguen cifrar los datos antes de enviarlos a la nube por 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](#) 

Autoevaluación

Las soluciones de CASB aportan una capa mas de detección de fuga de información

☒ Verdadero ☐ Falso

Verdadero

Este tipo de tecnología aporta más capacidad de detección ante varios tipos de situaciones de riesgo.

Los sistemas operativos móviles y las apps no suelen implementar controles para las compras integradas.

☐ Verdadero ☒ Falso

Falso

Tanto los sistemas operativos como las propias aplicaciones garantizan que el proceso de compras sea seguro mediante varios mecanismos, desde el cifrado de comunicaciones como el consentimiento del usuario.

Los empleados de una compañía suelen usar para acceder a los datos tanto terminales corporativos como los suyos propios personales.

☐ Verdadero ☒ Falso

Verdadero

Los usuarios usan tanto terminales corporativos como sus propios dispositivos personales, mezclándose el ámbito privado y el profesional.

Los sistemas de CASB es la solución definitiva para la fuga de información en entornos de nube.

☐ Verdadero ☒ Falso

Falso

No se puede hablar nunca en seguridad de soluciones definitivas, ya que cada vez los ataques son más avanzados, hay mas vulnerabilidades y los atacantes encuentran maneras de saltarse los controles establecidos.

