TIPOS DE APLICACIONES MÓVILES

AUTOR: ANGEL ALBERTO VARÓN QUIMBAYO

ÍNDICE

Introducción 3
Tipos de aplicaciones móviles 4
Sistemas operativos 7
Características de otros sistemas Operativos Móviles 9
Vulnerabilidades en las aplicaciones móviles 12
Amenazas a la privacidad del usuario 15
OWASP Mobile Security 18
Aplicaciones específicas en la empresa 20
Bibliografía 21

INTRODUCCIÓN

Las marcas y las empresas ya son conscientes de la necesidad de adaptarse a los dispositivos móviles. El consumo de los usuarios ha cambiado drásticamente en los últimos años, por lo que la información y las fuentes de ventas se apoyan de manera importante en los medios tecnológicos, sin embargo, a pesar de esta toma de conciencia, adaptar su negocio a la tecnología móvil, es un proceso que puede ser confuso - no sólo en términos de decisiones de marketing, sino también desde una perspectiva técnica, este último es aún más desconcertante cuando la terminología no es familiar.

Una de las primeras decisiones que los fundadores y gerentes de producto deben hacer cuando comienzan a centrarse en el móvil, es si van a hacer que su producto web sea "amigable" para pantallas móviles o que inviertan en desarrollar una aplicación móvil. En el primer caso, estamos hablando de sitios web o aplicaciones web de respuesta. En el segundo, nos referimos a aplicaciones para móviles que requieren descarga desde una tienda de aplicaciones, situación que plantea la siguiente pregunta: ¿Qué medidas se pueden tomar para brindar protección a las aplicaciones móviles y minimizar los riesgos?

Tipos de aplicaciones móviles

Una aplicación móvil es un programa que se puede descargar y al que puede acceder inmediatamente desde un teléfono o desde algún otro aparato móvil, hoy se tienen tres tipos de desarrollos para aplicaciones móviles: nativas, webs e híbridas que están sujetas a pruebas como el uso de emuladores y posteriormente dispuestas al mercado en un periodo estimado de prueba; a continuación, se explicará de qué se trata cada tipo.

Aplicaciones nativas: estas aplicaciones son creadas para ejecutarse en un dispositivo y sistema operativo específico, la mayor parte de las aplicaciones descargadas de App Store solo van a correr sobre iPhone e iPod. Estas aplicaciones son desarrolladas con distinto tipo de lenguaje, entre los cuales tenemos:

- Para el sistema iPad o iPhone (iOS) usan lenguajes objetive C, o C++.
- Para el sistema Android usan lenguaje Java.

Las aplicaciones nativas corren de forma eficaz sobre estos dispositivos, ya que, sus elementos se diseñan particularmente para el sistema operativo, pueden emplear todos los sensores y elementos del teléfono: GPS, cámara, agenda, etc. esta es una diferencia fundamental con respecto a las aplicaciones web.

El código fuente de las App se escribe en función del dispositivo, se compila a un ejecutable, comparable a un proceso de las tradicionales aplicaciones de escritorio. Los recursos como: imágenes e iconos, etc., que la aplicación requiere para ejecutarse van a ubicarse en un archivo compilado, que está listo para ser distribuido y subido a las App Store (tiendas de aplicaciones específicas del dispositivo).

Aplicaciones nativas

Ventajas	Desventajas
Utilización de los recursos tantos del sistema como del hardware.	Solo pueden ser utilizadas por un dispositivo que cuente con el sistema para el cual fue desarrollada.
Permite ser publicada en tiendas para su distribución	Requiere de un costo para distribuirla en una tienda, y dependiendo el sistema, para el uso del entorno de desarrollo.
En su mayoría, no necesitan estar conectadas a Internet para su funcionamiento.	Necesitan aprobación para ser publicadas en la plataforma.

Figura 1. Aplicaciones nativas
Fuente: propia

Aplicaciones web: se ejecutan desde un navegador en dispositivos con distintos Sistemas Operativos, el proceso de desarrollo es más sencillo, ya que, usa tecnologías conocidas, se genera código HTML, CSS, PHP y Java Script, y son interpretadas por un navegador.

Estas tecnologías y aplicaciones no requieren aprobación por parte de fabricantes para su publicación, estas aplicaciones Web pueden llegar a la misma apariencia que las aplicaciones nativas, dilatan en la capacidad que tienen las aplicaciones nativas para acceder a las características propias del dispositivo, tales como: el acceso a la cámara, teléfono o GPS.

Ventajas	Desventajas
Desarrollo sencillo y costo mínimo	Acceso limitado a hardware del dispositivo
Código reutilizable	Se requiere conexión a internet
No requiere instalación	Poca percepción en las tiendas

Figura 2. Ventajas y desventajas
Fuente: propia

Aplicaciones híbridas: las aplicaciones híbridas son una combinación de apps nativas con apps web y móviles, tienden a hacer las más usadas por permitir el uso de tecnologías multiplataforma como HTML, java script, CSS, admiten acceder a buena parte de los dispositivos y sensores del teléfono.

Gran parte de la infraestructura es tipo web y la comunicación con los elementos del teléfono se hace mediante comunicadores como Phonegap.

Claro ejemplo de ésta es Facebook que se descarga de la App Store y cuenta con todas las características de una aplicación nativa pero requiere ser actualizada ocasionalmente, al igual que las aplicaciones nativas, el código una vez creado se compila a un ejecutable, pero como en las aplicaciones web se genera código HTML, CSS y java script a ejecutar en un navegador. Ambos códigos se compilan mediante un paquete distribuible de la App Store.

Ventajas	Desventaja
Uso de los recursos del dispositivo y del sistema operativo	La documentación puede ser un poco escasa y desordenada.
El costo de desarrollo puede ser menor que el de una nativa	
Son multiplataforma	
Permite distribución a través de las tiendas de su respectiva plataforma	

Figura 3. Ventajas y desventajas.
Fuente: propia

Para el desarrollo de aplicaciones móviles se ha de tener en cuenta las limitaciones de estos dispositivos y considerar la gran variedad de tamaños de pantalla, datos específicos de software y configuraciones; por lo cual, han empezado a surgir páginas web donde el usuario puede crear aplicaciones sin ningún costo y sin poseer capacidad de programar, ejemplo de estas es: Mobincube.

Sistemas operativos

Son el software o los programas de proceso con rutinas de control, que administra los recursos que contiene el dispositivo, nos permite usarlo y darle órdenes para que haga lo que necesitamos.

Funciones:

- Abstracción del hardware.
- Compartir los recursos justamente.
- Proteger a todos los procesos de los demás procesos.
- Proteger a los datos de todos los usuarios de los demás usuarios.
- Asegurar la integridad de la información
- Los dispositivos móviles como teléfonos, tabletas y reproductores de mp3 son distintos, por eso sus sistemas operativos son más simples, orientados hacia la conectividad inalámbrica y a necesidades específicas.

Algunos sistemas operativos móviles son: Apple iOS, Google Android y Windows Phone.

Apple iOS: es un sistema operativo móvil de la multinacional Apple Inc. Originalmente desarrollado para el iPhone, después se ha usado en dispositivos de última generación como: el iPod touch, el iPad y Apple tv. No permite la instalación de iOS en hardware de terceros.

Sistema operativo ios	
Ventajas	• Fácil Configuración su mayor ventaja • Única plataforma(plataforma de código cerrado) • Gran almacén de aplicaciones disponible • Gran consistencia entre aplicaciones • Control por el fabricante en el software de aplicaciones, impidiendo la instalación de software dañino • Impermeable a virus y hackers virtualmente • No hay publicidad invasiva
Características	• Exclusivo de Apple • Sistema operativo fluido • Constantes actualizaciones • Añade voz a un mensaje de texto • Busca y edita rápidamente las fotos que se toman • Nuevas opciones de teclado y diferentes maneras de compartir contenido • Teclado más inteligente

Figura 4. Sistemas operativos IOS.
Fuente: propia

Android: es una plataforma o un sistema operativo para dispositivos móviles que contiene herramientas y aplicaciones dependiente de una distribución Linux, es de código abierto y fue desarrollada por Open Handset Alliance, por tal motivo, los desarrolladores pueden crear aplicaciones utilizando el SDK de Android escrito bajo Java, es uno de los sistemas operativos móviles más utilizados, por su fácil adaptación en cualquier dispositivo móvil.

CARACTERÍSTICA	SISTEMA OPERATIVO ANDROID
Kernel	Android depende de una versión de Linux para los servicios básicos del sistema como seguridad, gestión de memoria, gestión de procesos, apilamiento de red, y modelo de conductores. El núcleo también ejerce como una capa de abstracción entre el hardware y el resto del acoplamiento de software.
Aplicaciones	Las aplicaciones básicas incorporan un cliente de email, programa de SMS, calendario, mapas, navegador, contactos, y otros. Todas las aplicaciones son escritas en el lenguaje de programación Java.
Runtime	Android incluye un conjunto de librerías base que proveen la mayor parte de las funcionalidades disponibles en las librerías base del lenguaje de programación Java. Cada aplicación Android corre su propio proceso, con su propia instancia de la máquina virtual Dalvik, que ha sido escrito de forma que un dispositivo puede correr en múltiples máquinas virtuales de forma eficiente. (Deliverius). Dalkiv ejecuta archivos en el formato Dalvik Ejecutable (.dex), el cual está optimizado para memoria mínima. La Máquina Virtual está basada en registros, y corre clases compiladas por el compilador de Java que han sido transformadas al formato. Dex por la herramienta incluida "dx".
Framework de Aplicaciones	Los desarrolladores tienen acceso completo a los mismos Apis del framework usados por las aplicaciones base. La arquitectura está diseñada para simplificar la reutilización de componentes; cualquier aplicación puede publicar sus capacidades y cualquier otra aplicación puede hacer luego uso de esas capacidades (sujeto a reglas de seguridad del framework). Éste mismo mecanismo permite que los componentes sean reemplazados por el usuario. Una capa de servicios disponibles para las aplicaciones incluye: (Deliverius) Librerías: Android incluye un conjunto de librerías C/C++ usadas por varios componentes del sistema Android. Estas capacidades se exponen a los desarrolladores a través del framework de aplicaciones de Android. Algunas son: System C library (implementación librería C standard), librerías de medios, librerías de gráficos, 3d, SQLite, entre otras. (Deliverius)

Figura 5. Características de Android.
Fuente: propia

Windows Phone: sistema operativo móvil desarrollado por Microsoft, como sucesor de Windows Mobile. A diferencia de su predecesor está enfocado en el mercado de consumo en lugar del mercado empresarial. Con Windows Phone; Microsoft ofrece una nueva interfaz de usuario que integra varios de sus servicios propios como: OneDrive, Skype y Xbox Live en el sistema operativo.

Realizar un texto que introduzca el tema de ventajas y desventaja, el contenido no tiene hilaridad, cohesión y coherencia.

Ventajas	Desventajas
• Integración total con Windows • Sincronización del servicio de correo, OneDrive, contactos • Interfaz sencilla	• No alcanza al número de aplicaciones que se pueden disfrutar en Android o iOS • Baja posibilidad de personalización

Figura 6
Fuente: Propia

Características de otros sistemas Operativos Móviles

Antes de conocer algunos de los entornos descritos como IDE (entorno de desarrollo integrado) se debe conocer su concepto el entorno de programación, el cual está compactado como un programa de aplicación, es decir, radica en un editor de código, un compilador, un eliminador de fallas y un arquitecto de interfaz gráfica GUI.

Figura 7. Entornos de desarrollo móvil
Fuente: https://bit.ly/2JwPZqE

Los IDE cumplen con condiciones de interoperabilidad como: normas, especificaciones, protocolos, interfaces, etc. Pueden ser aplicaciones por sí solas o formar parte de una ya existente, permitiendo que el usuario, pueda usar cualquiera de estas y combinarlas según sus necesidades, mediante un navegador; no todos los IDE's son gratuitos.

Un IDE contiene ciertas características:

- Multiplataforma.
- Soporte para diversos lenguajes de programación.
- Integración con Sistemas de Control de Versiones.
- Reconocimiento de conexión.
- Extensiones y Componentes para el IDE.
- Integración con Framework.
- Depurador (eliminador de fallas).
- Importar y Exportar proyectos.
- Múltiples idiomas.
- Manual de Usuarios y ayuda.

Ventajas de los IDE's.

- La curva de aprendizaje es muy baja.
- Es más ágil y óptimo para los usuarios que no saben acerca del manejo de desarrollo móvil.
- Formateo de código.
- Funciones para renombrar variables, funciones.
- Warnings y errores de función en pantalla de algo que no va a interpretar o recopilar.
- Posibilidad de crear proyectos para poder ver los archivos gráficamente.
- Herramientas de reestructuración de códigos fuente.
- No es recomendado, pero posee un navegador web interno por si se quiere probar las cosas dentro de la IDE.

Los entornos de desarrollo móvil incluyen 4 elementos esenciales:

1. Datos: representación numérica, alfabética, algorítmica, espacial, etc. de un atributo o variable cuantitativa o cualitativa.
2. Metadatos: Son los descriptores de los datos.
3. Servicios: Son las funcionalidades accesibles por medio de un navegador que una IDE brinda al usuario para aplicar sobre los datos geográficos.
4. Aspectos organizativos: son normas y estándares que hacen que los sistemas puedan compartir y posibilitar intercambio de datos, leyes, reglas y acuerdos entre los productores de datos geográficos, así como el personal humano y la estructura organizativa.

Algunos de los entornos de desarrollo móvil se pueden agrupar con base en el lenguaje de programación.

Al enfocarse en el lenguaje de programación del lado del servidor es posible agrupar los IDE's así:

Lenguaje	Entorno IDE
PHP	Netbeans, Eclipse, Sublime Text, Aptana, Visual Studio Code, WebMatrix, Atom.
Java	Netbeans, Eclipse, Intellij.
.NET	Isual Studio Community.

Existen otros IDE's que utilizan editores de código, sobre todo HTML, donde al redactar un documento se va viendo el resultado final.

No se recomiendan ya que hay una dependencia directa de ese software y resultan demasiado pesados comparados con ciertos IDE's como Sublime Text o Atom, ejemplo de ellos, son: Dreamweaver, Kompozer y Bluegriffon.

En conclusión ciertos entornos son compatibles con múltiples lenguajes de programación, como: Eclipse o NetBeans, basados en Java o MonoDevelop, o en C++.

También puede integrarse la funcionalidad para lenguajes alternos mediante el uso de plugins. Por ejemplo, Eclipse y NetBeans tienen plugins para C, C++, Ada, Perl, Python, Ruby y PHP, entre otros, se recomienda estar atento en la evolución de los IDE's y de factores importantes como el desarrollo de aplicaciones, los beneficios, la distribución, la venta al por menor, la portabilidad y la fragmentación, entre otros.

Lectura recomendada

Se invita al estudiante a realizar la siguiente lectura

Informe sobre Seguridad Móvil y Riesgos de MobileIron Sistema de Gestión de la Seguridad de la Información

MobileIron

Vulnerabilidades en las aplicaciones móviles

Con el constante crecimiento de la sociedad informática, el afán de la sociedad del consumo, los constantes avances tecnológicos y el afán de los ciudadanos por adquirir dispositivos móviles, permite que los delincuentes informáticos desarrollen nuevas técnicas para atacar estos dispositivos.

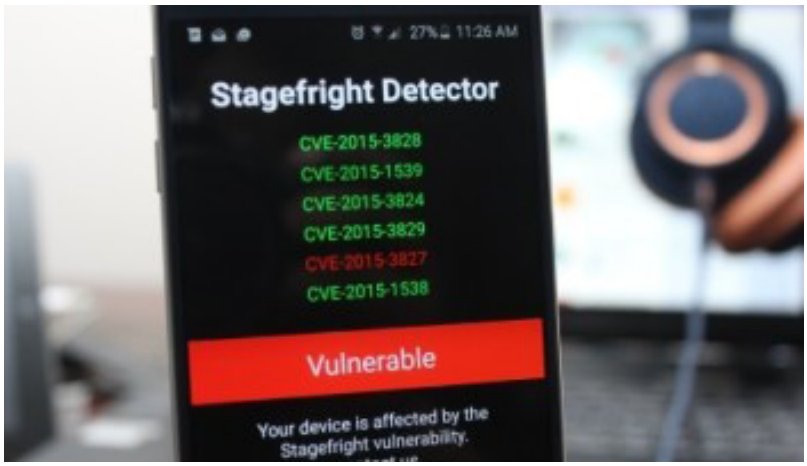

Figura 8. Factores que aumentan las vulnerabilidades en las aplicaciones móviles.
Fuente: https://bit.ly/2Pvp6J2

A todo esto, se suma la gran cantidad de usuarios desprevenidos, que usan los dispositivos móviles y sus aplicaciones, las cuales pueden ser inseguras y que se deben aplicar mecanismos de protección y prevención, lo que hace que se convierte en punto clave, ya que se facilita el ataque con un solo clic donde las vulnerabilidades están disponibles para los Ciberdelincuentes.

Esto facilita el trabajo de estos delincuentes permitiendo crímenes y desfalcar dinero de cuentas bancarias ligadas al dispositivo, convirtiéndose en un verdadero dolor de cabeza para nosotros los usuarios ya que estas acciones permiten el robo de datos hasta el hackeo total de nuestros dispositivos.

Hoy día los dispositivos móviles son el mayor objetivo de los hackers ya que el error que se comete es ingresar allí todos nuestros datos, si ingresamos desde cualquier red inalámbrica que se encuentre disponible, por lo cual, los usuarios nos encontramos más expuestos de manera virtual que real ya que no aplicamos las técnicas de seguridad necesaria y no se calculan las consecuencias de las acciones.

Snarfing o El bluesnarfing: es un delito informático reciente que consiste en introducirse en nuestro dispositivo móvil, por medio de un dispositivo cercano por medio de conexión bluetooth, sin que el usuario del móvil se percate, esto permite modificar, copiar y extraer información de nuestros dispositivos.

Bluejacking: es un novedoso delito electrónico que consiste en el envío de mensajes anónimos a dispositivos cercanos a través de bluetooth donde los atacantes se valen de

unas aplicaciones especializadas como es el caso del Bluetooth Messenger, el EasyJack y el Mobiluck.

La vulnerabilidad de los teléfonos móviles aumenta cuando se encuentran en modo "visible"; es decir, con la funcionalidad bluetooth disponible. El experto Marque Rowe aconseja a cualquier persona con un teléfono bluetooth mantenerlo en modo oculto puesto que al estar oculto el dispositivo, es más difícil de contactar.

A pesar de esto, en Internet hay aplicaciones apropiadas para descubrir y atacar dispositivos ocultos.

Otro de los factores que aumenta la vulnerabilidad en los dispositivos móviles son los virus informáticos que últimamente viene en aumento, según el diario el país, el Skulls (calaveras, en inglés), que como los anteriores se aprovecha de la confianza del usuario para instalarse en algunos terminales de Nokia, sustituyendo los iconos por tibias y cráneos, además de dejar inservibles todas las funciones menos la de envío y recepción de llamadas.

Otros virus conocidos para los dispositivos móviles son "Skulls". Que cuando se descarga y ejecuta el programa, reemplaza los iconos de su aplicación con el símbolo de la muerte (la calavera con dos huesos cruzados). También hace que la mayoría de los programas de bolsillo dejen de funcionar.

Por otra parte, hay algunos virus nuevos que se propagan solos. "Mabir", por ejemplo, se instala en el teléfono inteligente y espera a que lleguen mensajes de texto, cuando los recibe, envía una respuesta al remitente del mensaje de texto. El mensaje de respuesta incluye un archivo adjunto que contiene una copia del virus. Esto revela un desarrollo importante, ya que Mabir se propaga de manera muy similar a la de los gusanos comunes, que tiene la capacidad de enviarse a sí mismo desde un teléfono infectado a otros teléfonos inteligentes compatibles.

El Pishing, según explica Marco De Mello, fundador de la empresa de seguridad informática PSafe, es una técnica que busca obtener: datos, contraseñas, claves de acceso, números de identificación personal o llaves maestras digitales que el propio usuario otorga a los hackers al entrar en un enlace apócrifo que, usualmente, se disfraza de sitio auténtico.

En pocas palabras, el Pishing se basa en un enlace que funciona como el cebo utilizado para pescar, y he ahí la razón de su nombre y la importancia de crear buenos hábitos virtuales como lo son:

- usar una contraseña distinta para cada cuenta en especial de uso bancario.
- abstención de ingresar a links enviados por correo o redes sociales.
- verificar cada vez que sea posible que quien dice haber enviado el mensaje en verdad lo sea.

Crear buenos hábitos y ser precavidos en línea es un tema difícil, pero es muy necesario en entornos digitales, hay que mantener atentos a todo lo que nos aparece en las pantallas de nuestros móviles, a pesar de las inversiones para el software y licencias de seguridad, la vulnerabilidad principal recae en los usuarios.

Otra de las vulnerabilidades que son poco visibles son las plataformas como lo son los Sistemas Operativos, Servidores y Bases De Datos, que últimamente han sido cuestionados por la gran cantidad de fallos que presentan permitiendo el incremento de la vulnerabilidad lo que ha permitido la propagación de virus informáticos.

Video

Se recomienda ver el siguiente video:

Vulnerabilidad en las aplicaciones móviles

https://goo.gl/wSjFwq

Figura 9. Virus
Fuente: https://bit.ly/2zkINKo

Instrucción

Se invita al estudiante a revisar el recurso de aprendizaje: infografía.

Amenazas a la privacidad del usuario

La capacidad de los sistemas informáticos y aplicaciones junto a la acumulación de datos de carácter personal por entidades públicas y privadas, gestan claras amenazas a la privacidad de los usuarios.

A continuación, se muestran las amenazas más destacadas de los últimos años que afectan al usuario según los especialistas del laboratorio de investigación de ESET Latinoamérica, quienes manifiestan que existen nuevos códigos Maliciosos, para vulnerar y violar la privacidad de los dispositivos móviles.

Privacidad en Internet: los servicios que se ofrecen por medio de estos dispositivos móviles, presentan algunas fallas originadas desde el diseño de los mismos, los ciberdelincuentes aprovechan estas vulnerabilidades y hackean los equipos para la recopilar información Confidencial, Como ejemplo tenemos uno de los casos ocurridos haces pocos meses, por medio de Facebook, en el cual 6 millones de usuarios vieron su información expuesta, y Twitter con 250.000 usuarios comprometidos.

- Redes inalámbricas (WiFi, bluetooth o infrarrojos) Los atacantes pueden utilizar puntos de acceso falsos y engañar al dispositivo para que se conecte automáticamente a una red de supuesta confianza desde dónde se vigila la actividad del usuario sin que éste sea consciente de ello.

- Ransomware (del inglés ransom, 'rescate', y ware, por software) es decir Secuestro de información donde se utilizan diferentes aplicaciones maliciosas que realizan esta práctica de diferentes formas, este tipo de malware tiene la cualidad de traducir archivos en el dispositivo del usuario contagiado, ya sean de tipo texto, hojas de cálculo, fotos o videos. Para luego solicitar dinero para poder acceder nuevamente a la información personal. En américa latina se reveló el tema de un troyano denominado Multi Locker, el cual era controlado desde un Centro de Comando y Control (C&C).

- Rodpicom: uno de los casos más recientes en que se aplicó Ingeniería Social y que por medio de sus técnicas permitió la propagación de este gusano o código malicioso que se propagó rápidamente enviando mensajes a los contactos de Skype y Gtalk de un usuario infectado. Al dar clic en el enlace este descargaba una presunta imagen en el dispositivo, y resultaba ser un ejecutable malicioso. Dejó huella ya que logró afectar a más de 300 mil usuarios a unas pocas horas desde que inició.

- Servidores vulnerables y troyanos bancarios: El Laboratorio de Investigación de ESET Latinoamérica detectó un código malicioso que se propagaba a través de una campaña de spam, el cual instalaba un plugin de Google Chrome para interceptar todas las páginas web que navegaba la víctima, en búsqueda de sitios web bancarios pertenecientes a entidades financieras de Brasil. Además, el código malicioso utiliza un servidor gubernamental legítimo de ese país (que contenía un error de diseño) para el envío de la información. Se trató de una amenaza avanzada con la potencialidad de afectar a muchos usuarios.

- las cookies, los cuales son archivos de texto que pueden recoger toda la información sobre los movimientos del usuario en Internet, "capturando" datos como: sus hábitos, poder de compra, domicilio, cargas familiares, etc.

- El Pishing, existen cinco formas de éste:

1. Pishing tradicional: falsificación de un solo sitio frecuentado por el usuario para obtener datos.

2. Pishing redirector: usa dos o más sitios que el tradicional para proceder a la estafa.

3. Spear Pishing: usa correos personificados, falsifican direcciones empleados de compañías con perfiles determinados.

4. Smishing SMS: se usa un canal digital ejemplo: teléfonos celulares, whatssapp o telegram, enviando mensajes de texto informando que se es ganador de un premio, donde la víctima debe responder a través de un código, número, llamar a falsas líneas de atención Donde piden datos personales para hacer válido su premio, su principal meta es obtener un crédito bancario.

5. Vishing: como la anterior falsedad de líneas de atención donde realizan las falsas llamadas, este tipo de Pishing se une a otro para complementar credibilidad haciendo más fácil el fraude.

Otras amenazas

- El caso de Cdorked, un backdoor que afectó a más de 400 servidores web de Apache, Lighttpd y nginx, muchos de ellos de sitios populares.

- una falsa aplicación de Adobe Flash que se propagó por Google Play y que realmente era un tipo de malware que buscaba recopilar información sensible del usuario.

- Malware de 64 bits, éste ha visto un crecimiento durante este año; en la región, México y Perú países de Latinoamérica más afectados por malware de 64 bits.

- Curiosidad del usuario: los atacantes logran a través de premios, promociones, ofertas de empleo, un ¿quieres saber quién ha visitado tu perfil en Facebook? o conversaciones espiadas en whatsapp llegar a los usuarios y así atacar pues detrás de estas tácticas se encuentran los malware llevando a que más usuarios sean engañados, con la inclusión de la tecnología también los usuarios menores tienen disponible el acceso a internet y redes sociales desde cualquier plataforma móvil e inclusive en el colegio lo cual ha llegado en algunos casos a fatídicas consecuencias pues son aún más vulnerables

Vulnerabilidades específicas de los entornos de aplicaciones móviles.

El entorno móvil se ha ido ampliando y la tendencia de crecimiento va de la mano con la inclusión de nuevos dispositivos con conectividad y con sistemas operativos móviles propios, en la actualidad es común ver cómo estos sistemas están siendo ana-

lizados y atacados, sus riesgos y vulnerabilidades, dejan gran preocupación con respecto a la seguridad.

Las vulnerabilidades que generan mayor preocupación en cuanto a los dispositivos móviles, son:

- el uso no autorizado de los dispositivos para realizar actividades como monitoreo de actividades, recuperación y sustracción de datos e información, marcación, envió de mensajes y pagos no autorizados, suplantación de interfaces y usuarios. Modificación del sistema, procesamiento a terceros almacenamiento de información sin permiso, ataques a otros usuarios o sistemas, rastreo no autorizado de los dispositivos, seguimiento de usos, destrucción del hardware.

Entre muchas otras actividades no permitidas por los usuarios y por las autoridades competentes en el tema de seguridad.

La siguiente gráfica muestra los perímetros porosos de la seguridad informática enfocada en los dispositivos móviles.

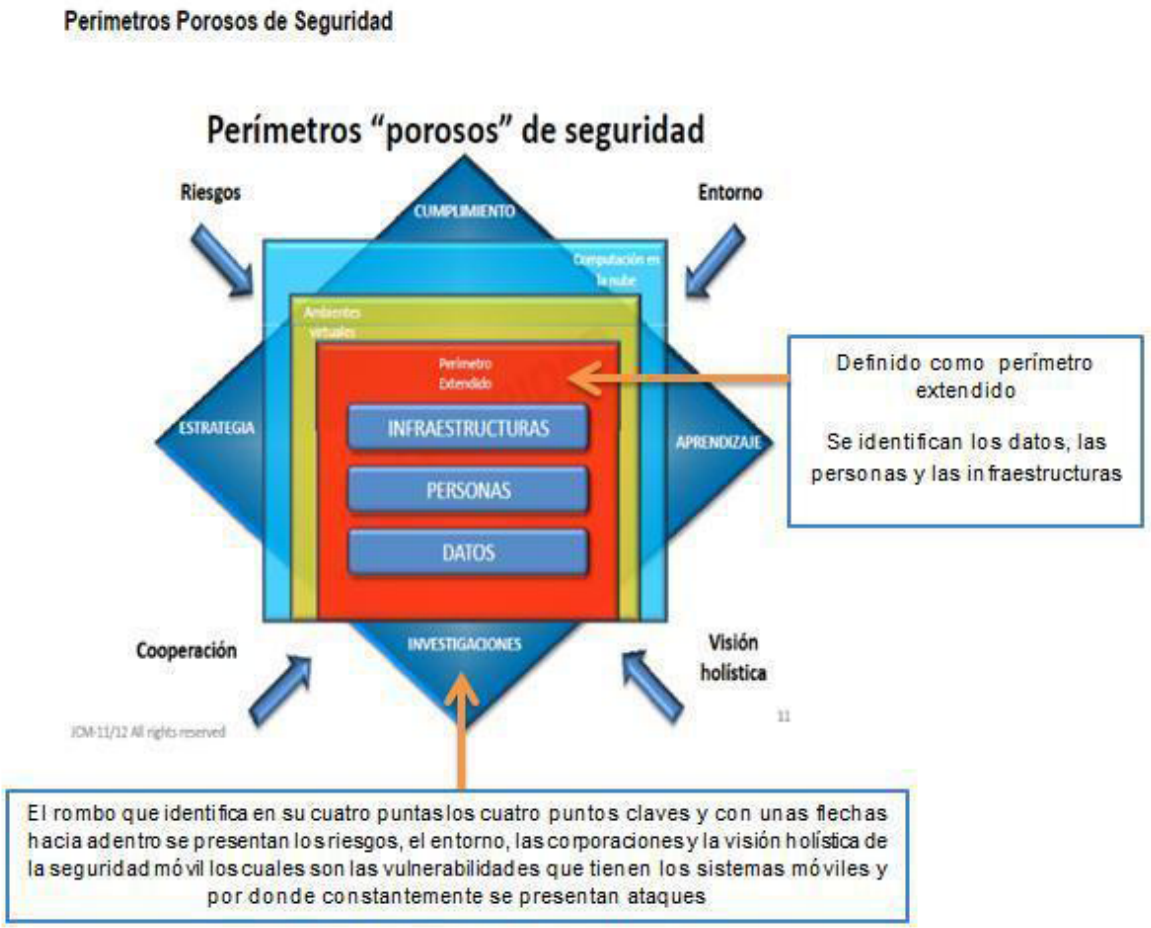

Figura 10. Perímetros porosos de la seguridad.
Fuente: Propia.

Video

Se recomienda ver el siguiente video:

Seguridad en aplicaciones

https://vimeo.com/240860703

Se invita al estudiante a realizar la siguiente lectura

Seguridad en Aplicaciones Móviles

Molina, F.

OWASP Mobile Security

El proyecto OWASP móvil nos indica que es indispensable que el diseño de la aplicación a desarrollar se modele con algunas amenazas, esta técnica permite detectar la vulnerabilidad para almacenar datos seguros, esto ayuda a interpretar los activos de información que se procesa y cómo las APIs ocultas manipulan dichos activos, ya que estas API deben almacenar información privada de forma segura.

Estos son algunos de los sitios que OWASP, observa que con mayor reiteración almacenan los datos de forma insegura:

- Bases de datos SQLite.
- Archivos de registro.
- Archivos Plist.
- Almacenes de datos XML o archivos de manifiesto.
- Almacenes de datos binarios.
- Tiendas de galletas.
- Tarjeta SD.
- Nube sincronizada.

Al aplicar encriptación y descifrado a activos de información confidenciales, el malware puede realizar un ataque binario en la aplicación para robar claves de cifrado o descifrado. Una vez que roba las claves, descifrará los datos locales y robará información confidencial.

¿Qué hacer para prevenir el almacenamiento inseguro de datos?

La base fundamental para el desarrollo de aplicaciones móviles, consiste en evitar almacenar datos a menos que sea exclusivamente necesario. Como desarrollador debe aceptar que los datos se pierden en cuanto toca el móvil. Por eso es necesario reflexionar sobre las implicaciones de perder datos de los usuarios de móviles mediante kernels modificado jailbreak o exploit de raíz silencioso aprovechando una parte de datos o secuencia de comandos y/o acciones, utilizada con el fin de vulnerar la seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

OWASP recomienda investigar sus API de seguridad de datos de plataformas y asegurándose de que las está llamando apropiadamente. La lección aquí es saber qué datos se están almacenando y protegerlos apropiadamente.

Almacenamiento de datos inseguros

- Espía de amenaza detallada de la aplicación: Los espías de amenazas
- Incluyen lo siguiente: un enemigo que ha localizado un dispositivo móvil

que se ha perdido / robado; se utiliza una aplicación maliciosa, Malware o aplicación encriptada que actúa en nombre del oponente y que se ejecuta en el dispositivo móvil.

- Vector de ataque: es el método que utiliza una amenaza para atacar un sistema, en caso de que un adversario alcance físicamente el dispositivo móvil, esté conecta el dispositivo móvil a una computadora con software libre que se encuentra disponible en la web, utilizando esta aplicación puede alcanzar todos los directorios de software de terceros que por lo general contienen información personal y fácil de identificar u otros activos de información privada.

- Un Ciber delincuente puede construir malware o modificar una aplicación legítima para robar tales activos de información.

- Debilidad de seguridad: esto ocurre cuando los espacios de almacenamiento de datos son frágiles y los desarrolladores de la aplicación creen estar seguros de que los códigos maliciosos no podrán acceder al dispositivo móvil, menos a los almacenes de datos del dispositivo.

- Impactos técnicos: la falla técnica para el almacenamiento de datos inseguro puede ocasionar pérdida de información.

Lista de datos vistos y almacenados, que se constituyen en piezas valiosas:

- Nombres de usuario.
- Registro de autenticación.
- Contraseñas.
- Cookie.
- Datos de localización.
- UDID / EMEI, Nombre de dispositivo, Nombre de conexión de red.
- Información Personal: DoB, Dirección, Social, Datos de Tarjeta de Crédito.
- Datos de la aplicación.
- Registros de aplicaciones almacenadas, por ejemplo, para un Android Apps ADB logcat.
- Información de depuración.
- Mensajes de aplicación almacenados en caché.
- Historial de transacciones.

Instrucción

Se invita al estudiante a revisar la actividad de aprendizaje: control de lectura.

Aplicaciones específicas en la empresa

Las vulnerabilidades de almacenamiento de datos inseguros suelen dar lugar a los siguientes riesgos que la organización debe contrarrestar mediante aplicación de políticas de seguridad:

- El robo de identidad
- Fraude
- Daño de reputación
- Violación de políticas externas (PCI) O Pérdida de material

Top de Almacenamiento de datos Inseguros

Figura 11. Almacenamiento de datos inseguro M
Fuente: https://www.owasp.org/index.php/Mobile

Cierre

Es importante reconocer las múltiples ventajas y facilidades implícitas en los dispositivos móviles, sin embargo, debido a su amplia masificación y uso general, los usuarios se exponen constantemente a los diferentes riesgos asociados a esta tecnología, como daños, pérdidas, uso de wifi públicas, por tanto, desde el diseño y el desarrollo de aplicaciones, se deben agregar elementos para garantizar un esquema de seguridad que cumpla con los estándares. A continuación, se invita al estudiante a realizar la actividad evaluativa.

BIBLIOGRAFÍA

Aguilar, L. (2011). Computación en la nube: estrategias de Cloud Computing en las empresas. España: Editorial Marcombo.

Carrasco, R. (2011). Seguridad en Aplicaciones, Redes y Sistemas Informáticos. Editorial Librería Bubok.

Carrera, E. (2010). El Costo de la Seguridad en Dispositivos Móviles. Recuperado de https://revistas.ute.edu.ec/index.php/eidos/article/view/65

Fisher, R. (2010). Seguridad en los sistemas informáticos. Madrid España: Ediciones Díaz de Santos.

Santos, J. (2010). Seguridad informática. RA-MA S.A. Editorial y Publicaciones.

Hernández, L., Carreto, C., y Mechaca, R. (2012). Modelo de Seguridad para Redes Aplicado a Dispositivos Móviles. Recuperado de http://repositoriodigital.ipn.mx/bitstream/123456789/8159/1/RISCE%20-%20Enero%202012.pdf#page=17

MobileIron. (2016). Informe sobre Seguridad Móvil y Riesgos de MobileIron. Recuperado de https://info.mobileiron.com/rs/049-OIH-745/images/security-report-Q216-v1.5.1-ES-A4.pdf?aliId=96100995

Molina, F. (2012). Seguridad en Aplicaciones Móviles. de http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/Fabian_Molina_VIJNSI.pdf

Pakala, S. (2010). Preguntas Frecuentes sobre Seguridad en Aplicaciones Web (OWASP). Editorial OWASP The Open Web Aplication Security Proyect.

Symantec. (2017). Application security mobile networks. Recuperado el 12 de 03 de 2018, de http://www.symantec.com/es/mx/theme.jsp?themeid=application-security-mobile-networks

Varón, A. (2011). Hacking y seguridad en internet . Ra-Ma Editorial, S.A.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica