ARTÍCULO 2

Metodología para seguridad de ataques a dispositivos móviles

Camana, Carlos[1]
[1]Instituto Superior Tecnológico Bolívar, Ambato, Ecuador

Resumen: Hoy en día las personas que hacemos uso de los diversos dispositivos móviles requieren de información en tiempo real para cumplir distintas necesidades a través de apps, pero éstas pueden ser vulnerables y sujetas a amenazas informáticas, por lo que, se requieren de medidas de protección para mitigar potenciales ataques cibernéticos. En este sentido, la seguridad móvil es cada vez más importante, tanto para usuarios personales como empresariales, sumado con el crecimiento del Internet de las Cosas (IOT), la seguridad en especial de nuestros teléfonos inteligentes se vuelve cada vez más relevante, por lo tanto, es importante apoyarse de una metodología para la validación de herramientas de seguridad dirigida a usuarios de dispositivos móviles y evitar que las amenazas que atentan contra la seguridad como: malware, fuga de información, vulnerabilidades de software, ingeniería social entre otras se materialice.

Palabras clave: ciberseguridada, amenazas, vulnerables, ataques.

Methodology for security of attacks to mobile devices

Abstract: Nowadays, people who make use of different mobile devices require information in real time to meet different needs through apps, but these can be vulnerable and subject to computer threats, so protection measures are required to mitigate potential cyber attacks. In this sense, mobile security is increasingly important, both for personal and business users, coupled with the growth of the Internet of Things (IOT), security especially of our smartphones is becoming increasingly relevant, therefore Therefore, it is important to rely on a methodology for the validation of security tools aimed at users of mobile devices and prevent threats that threaten security such as: malware, information leakage, software vulnerabilities, social engineering, among others, from materializing.

Keywords: cybersecurity, threats, vulnerable, attacks

1 INTRODUCCIÓN

En los últimos años, específicamente en la telefonía móvil se ha experimentado una amplia evolución a tal punto de llegar a características similares a las de una laptop.

Estos Smartphone permiten conectarse a Internet y acceder a redes sociales, navegar en la web, acceder a los correos electrónicos, ejecutar trámites bancarios o comerciales, entre otros. Para lo cual, estos dispositivos necesitan de un sistema operativo instalado como: Android, iOS (iPhone), Windows Mobile y Phone, BlackBerry, Symbian; entre otros.

Estos sistemas operativos presentan a su vez una gran variedad de vulnerabilidades (fallos) por lo que, el programa Common Vulnerabilities and Exposure (CVE) identifica estas vulnerabilidades cada año como se presenta en el siguiente grafico estadístico del aña 2019.

Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2019

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	414
2	Debian Linux	Debian	OS	360
3	Windows Server 2016	Microsoft	OS	357
4	Windows 10	Microsoft	OS	357
5	Windows Server 2019	Microsoft	OS	351
6	Acrobat Dc	Adobe	Application	342
7	Acrobat Reader Dc	Adobe	Application	342
8	Cpanel	Cpanel	Application	321
9	Windows 7	Microsoft	OS	250
10	Windows Server 2008	Microsoft	OS	248
11	Windows Server 2012	Microsoft	OS	246
12	Windows 8.1	Microsoft	OS	242
13	Windows Rt 8.1	Microsoft	OS	235
14	Ubuntu Linux	Canonical	OS	190
15	Fedora	Fedoraproject	OS	184
16	Chrome	Google	Application	177
17	Linux Kernel	Linux	OS	170
18	Iphone Os	Apple	OS	156
19	Leap	Opensuse	OS	146
20	Sd 625 Firmware	Qualcomm	OS	145

Figura 1: Top Vulnerabilidades en SO
Fuente CVE - 2019

Los ataques a los dispositivos móviles se dan en su mayoría por medio de apps maliciosas, por eso, en el sistema operativo Android (SO con más vulnerabilidades y más utilizado en el mundo) se pueden instalar directamente apps, razón por la cual conectarse a Internet es exponerse a peligros, pues está considerado que, los ataques a estos dispositivos generan más dinero que los realizados a otros (computadores, servidores, etc.).

2 MARCO TEÓRICO / METODOLOGÍA

Amenaza, vulnerabilidad, ataques ciberseguridad.

Las **amenazas** de seguridad de la información son como un potencial evento de afectar negativamente, es decir por un acceso no autorizado a un sistema de información se puede materializar la divulgación, destrucción, modificación y/o la denegación de servicio".

En cambio, una **vulnerabilidad** se considera como la debilidad de un procedimiento de un sistema de información, misma que podría explotarse intencional o accidentalmente para violentar controles o políticas de seguridad de dicho sistema.

En otras palabras, las amenazas figuran como un potencial de daño, mientras que las vulnerabilidades implican una condición para que se materialice el daño.

En **Ciberseguridad**, los **ataques** son mecanismos por el que un actor (hackers) explota una vulnerabilidad para causar un daño y afecte a la confidencialidad, integridad o disponibilidad de un sistema de información.

Amenazas

Entre las amenazas más comunes podemos encontrar en dispositivos móviles con SO Android son las siguientes:

Ransomware.- Actúan cifrando los archivos para que el usuario no pueda acceder a ellos y a cambio le pide realizar un pago como rescate.

Adware.- Aplicaciones que realizan falsos clics en publicidad sin el consentimiento de los usuarios; por ejemplo, el usuario está jugando y al hacer clic en la pantalla de forma encubierta también hace un clic en una publicidad.

Troyanos.- Son apps aparentemente legítimas e inofensivas, pero que al ejecutarlas brindan al atacante un acceso remoto al móvil, proporcionan una puerta trasera al dispositivo que permite ejecutar código malicioso e infectarlo.

Keyloggers.- Son programas que se ocultan en apps para guardar registros de las pulsaciones de las teclas que se da en la pantalla del dispositivo móvil.

Troyanos bancarios.- Se presentan a través de una app en apariencia similar a la de un banco, (clonada). Con estas apps, los atacantes se apropian de información relacionada con sus cuentas bancarias.

APT (Advanced Persistent Threat).- Es un tipo de ataque que se caracteriza por combinar varias vulnerabilidades, los atacantes utilizan perfiles falsos en redes sociales para conseguir engañar y chatear con sus víctimas y direccionarlas para que se instalen apps con las cuales infectan el móvil con un troyano, o un ransomware.

Ataques

Enfoque técnico.- Como ejemplo de un ataque a un dispositivo móvil que permita espiar a usuarios con SO Android podemos citar el ataque a los procesadores Qualcomm Snapdragon, que se utilizan en más del 40% de los smartphones en todo el mundo.

Este elemento conocido como Procesador de Señal Digital (DSP), forma parte de los móviles Android, incluyendo dispositivos de marcas como: Google, Samsung, Xiaomi o LG. Según expertos, el DSP presenta varias vulnerabilidades que los cibercriminales sacan provecho para espiar a personas mediante su teléfono móvil.

El DSP es un sistema implementado para captura de imágenes y vídeos, utilización de realidad aumentada o el reconocimiento de voz, además se encarga de procesar señales en tiempo real, como la conversión de señales de voz, video en datos computables.

Un DSP contiene los siguientes componentes claves:

- Memoria de programa: Almacenamiento de programas para procesar los datos.
- Memoria de datos: Acumula información a procesar.
- Motor de cálculo: Realiza el procesamiento matemático, accediendo a la memoria de programa y datos
- Entrada / Salida: Proporciona una amplia variedad de funciones para conectarse con el mundo exterior.

Por estas funcionalidades un DSP se ha convertido en uno de los vectores de ataque más novedosos y utilizados, pues aumentan las posibilidades de ser atacado.

Para poder explotar estos fallos de seguridad, los atacantes necesitarían que el usuario se descargue e instale una aplicación que no requiere permisos y que es aparentemente fiable. Así, podrían acceder al teléfono y poder:

Transformar el smartphone en una herramienta de espionaje: Usar el teléfono de la víctima para espiarla sin necesidad de interacción con el usuario. Acceda a la información como fotografías, vídeos, localización o GPS y también podría grabar llamadas e incluso activar el micrófono.

Interrumpir funcionamiento: Conseguir que el móvil de la víctima no funcione como de costumbre, haciendo que toda la información almacenada no esté disponible.

Hacer actividades maliciosas: Ocultar malware que evita detectar las actividades maliciosas que el cibercriminal esté realizando desde el teléfono.

Es importante acotar que estos programas maliciosos en la mayoría de casos no se pueden eliminar.

Metodología de seguridad

Para determinar una metodología de seguridad en dispositivos móviles, se debe tomar en cuenta los principales principios sobre la seguridad de la información:

- **Confidencialidad.-** Los datos sólo deben leídos por usuarios previstos y autorizado, no se revelará a terceros salvo cuando sean autorizadas.
- **Integridad.-** Los datos sólo deben ser actualizados por usuarios previstos y autorizados, es decir los datos se deben mantener intactos y libre de modificaciones por terceros.
- **Disponibilidad.-** Usuarios autorizados deben ser capaces de acceder a sus datos. Entendemos aquella información a la que podemos acceder cuando la necesitamos a través de los canales adecuados y autorizados.

En tal virtud, se deben adoptar buenas prácticas que se debe llevar a cabo para asegurar sus dispositivos móviles. Estas están destinadas a proporcionar protección contra los ataques latentes:

Política Screen-lock (Bloqueo de Pantalla)

Configurar la pantalla mediante bloqueo por PIN, patrón de puntos, contraseña o biometría es una característica común en los dispositivos móviles para aumentar la seguridad del usuario, proporcionando un mecanismo de autenticación para tener acceso a los contenidos del dispositivo.

Esto evitará que usuarios no autorizados tengan acceso, mejorando así significativamente la confidencialidad e integridad de los datos del usuario.

Cada método de bloqueo depende de cada SO tenga. La longitud del PIN, la cantidad de puntos de un patrón, la cantidad de caracteres y tipos de una contraseña determinarán cuan seguro y robusto será el método.

Bloqueo remoto, tracking y borrado de la información

Una manera eficaz de proteger la confidencialidad e integridad de los datos es mediante un método de borrado remoto que se trata de realizar un seguimiento geo posicional del dispositivo con una política de limpieza, esto permitirá que un usuario pueda activar de forma remota el bloqueo del dispositivo, conocer la ubicación del mismo o iniciar un borrado que elimine todo el contenido.

Un ejemplo de estas funcionalidades es la herramienta provista por Android llamada "Android Device Manager"; esta herramienta viene integrada en todos los dispositivos Android y brinda 4 funcionalidades:

1. Hacer sonar el dispositivo.
2. Localizar el dispositivo (depende que el dispositivo tenga la localización activada).
3. Bloquear el dispositivo.
4. Borrar el dispositivo (tiene algunas limitaciones respecto a la tarjeta SD).

Se accede mediante una cuenta de Google que se registra en el dispositivo entrando a: "https://www.google.com/android/find"

Encriptación o cifrado de datos

En seguridad móvil implica principalmente dos tipos de cifrado: cifrado del dispositivo y cifrado de red.
El cifrado de dispositivo es la encriptación de los datos almacenados, utiliza para proteger los datos de texto. Aunque un atacante se haga con los datos almacenados le será es inútil ya que no podrá leerlos.

Dependiendo del esquema de cifrado y de su robustez, (DES, RSA, AES, etc.) el resultado de aplicar un cifrado del almacenamiento del dispositivo será prevenir o retrasar a un atacante.

En cambio, el cifrado de red proporciona protección durante el transporte a través de redes no confiables como Internet. El protocolo de transferencia de hipertexto seguro (HTTPS) y de red privada virtual (VPN) son ejemplos de protocolos y servicios que pueden ser utilizados para cumplir este nivel de seguridad y evitar el espionaje y la fuga de datos.

Control de aplicaciones

Actualmente se ofrece una amplia gama de dispositivos móviles de varios fabricantes con diversas versiones de sistemas operativos, mismos que se deben configurar para no permitir instalaciones de aplicaciones que se distribuyen desde un tercero y sólo permiten las que se distribuyen desde una plataforma oficial.

A la hora de buscar una aplicación en los repositorios oficiales se debe realiza un análisis que implica la revisión de código de contenido malicioso que pretende ingresar. Sin embargo, los repositorios oficiales no están completamente libres de peligros por lo cual siempre es recomendable realizar una revisión de las aplicaciones antes de instalarlas.

Una revisión simple es tener en cuenta los permisos que la aplicación solicita para funcionar, por ejemplo, una aplicación para usar el led del flash del dispositivo como linterna, si a la hora de instalar ésta solicitara permisos para usar el GPS, realizar llamadas o acceder a datos de navegación, el usuario tiene un claro indicador para sospechar que esta aplicación tiene intencionalidades diferentes a las que informa.

Técnicas y Aplicaciones para reforzar la seguridad

Los **Antivirus** de dispositivos móviles cumplen la misma función que en las PCs, realizan escaneos de las aplicaciones instaladas, mantienen una base de datos de las aplicaciones maliciosas conocidas regularmente, brindan funcionalidades para la eliminación de malware, el control de tráfico de red, bloqueo de aplicaciones, dispositivo, bloqueo remoto, firewall, entre otros.

Las **Vaults** o bóvedas, son aplicaciones que por su funcionalidad de cifrar y proteger proveen un almacenamiento más seguro dentro del dispositivo móvil.

Las funcionalidades más comunes son: galerías privadas, fotografía en caso de contraseña incorrecta (si se ingresa una contraseña incorrecta se hace uso de la cámara frontal para sacar una foto de quien intentó acceder y la almacena en la vault), bloqueo de aplicaciones con contraseña, copias de seguridad en la nube, etc.

3 RESULTADOS Y DISCUSIÓN

Con lo descrito, podemos decir que, cuando usamos un dispositivo móvil con internet, estamos expuestos a cualquier ataque en la que se vea comprometida nuestra información.

Por lo tanto, debemos estar siempre atentos y actualizados para poder mitigar en lo mínimo cualquier amenaza, sobretodo cundo estemos trabajando en internet.

La mayoría de usuario en especial jóvenes, existe la tendencia de instalar nuevas y desconocidas aplicaciones ya sea por curiosidad o por una preferencia de redes sociales; pero que no tienen presente de los ciberataques que pueden ser víctimas.

Common Vulnerabilities and Exposures, (CVE), provee una lista anual de vulnerabilidades de seguridad, en la que codifica con un número CVE-ID, describe el fallo, informa de una posible solución si existe o como mitigarla.

4 CONCLUSIONES

- Con las distintas formas de ataque informáticos a la que estamos expuestos, de debe seguir fomentando y divulgando las buenas prácticas en seguridad móvil en la sociedad.
- También existe una gama de aplicaciones móviles que el usuario puede hacer uso para apoyarse y proteger su información personal y no ser víctima de cualquier forma de ataque intencional.
- La seguridad de los dispositivos móviles constituye una problemática actual de gran interés, a la hora de diseñar e implementar soluciones y gestionar la seguridad de los dispositivos se debe abordar la problemática en forma integral, es decir una implementación de políticas, normas y procedimientos que contribuyas a tener nuestros datos seguros.

5 REFERENCIAS

Engebretso, P. (2018). The Basics of Hacking and Penetration Testing. USA, Cengage

Erickson, J. (2019). Hacking: The Art of Exploitation. USA, Arte Público Press

Pacheco, v. (2017). Estudio y análisis de seguridad en dispositivos móviles. Seguridad Informática, 15.

Guzmán, J. (2013). Análisis de vulnerabilidades de dispositivos móviles. Seguridad SO. 18

CVE, Common Vulnerabilities and Exposures Obtenido de: https://cve.mitre.org/ (Diciembre, 2019)

EFE, Agencia de noticias internacional Obtenido de: https://www.efe.com/efe/espana/politica/la-moncloa-y-el-cni-investigan-hackeo-de-moviles-ministros-altos-cargos/10002-4330865 (Agostos, 2020)