Universitat Oberta de Catalunya

Universitat Autònoma de Barcelona

UNIVERSITAT ROVIRA i VIRGILI

Universitat de les Illes Balears

PRESENTACIÓN

Seguridad en Smartphones: Análisis de riesgos de vulnerabilidades y auditorías de dispositivos

Título: Presentación del TFM, Master Interuniversitario en Seguridad de las TIC

Autor: Carlos García Altarejos, carlosg.altarejos@gmail.com, charly84@uoc.edu

Tutor: Marco Antonio Lozano Merino, mlozanome@uoc.edu

Fecha: 12 de enero de 2017

INTRODUCCIÓN

Con el presente trabajo se pretende desarrollar una metodología para realizar un análisis de riesgos de vulnerabilidades y auditorias de dispositivos, que pueda servir para prevenir estas amenazas y protegerse frente a ellas. El principal objetivo se centra en el estudio de las herramientas y técnicas para detectar las amenazas y las vulnerabilidades que afectan a estos dispositivos.

La metodología está estructurada en cinco fases que son: identificación, análisis, acceso, resultados e informe. Con estas se pretende poder llevar a cabo un análisis para identificar e informar fallas en los dispositivos y en los procesos tecnológicos. Enfocado a la protección total de los recursos que estén expuestos a posibles amenazas de seguridad informática.

Este tipo de análisis no suele incluir, las etapas relacionadas con la explotación de las vulnerabilidades identificadas, sino que solo trabaja sobre la correcta identificación de las mismas. Los sistemas operativos móviles que se estudiarán son Android(Google) e IOS(Apple).

Por último, en las distintas fases de este proyecto se estudian y analizan herramientas de tipo comercial y Open Source, que serán de gran utilidad a la hora de realizar los análisis sobre los correspondientes dispositivos móviles.

A continuación desarrollaremos un breve resumen del TFM, describiendo los diferentes apartados de los que consta este proyecto.

PLAN DE TRABAJO

Propósito y objetivos

El plan de trabajo es la primera parte del proyecto, donde definiremos el propósito de este y los objetivos a lograr.

Con el presente trabajo se pretende desarrollar una metodología para realizar un análisis de riesgos de vulnerabilidades y auditorias de dispositivos, que pueda servir para prevenir amenazas y protegerse frente a ellas. Este propósito surge debido a la proliferación de los smartphones y de su uso generalizado en el ámbito profesional y particular, para garantizar la seguridad de la información.

El principal objetivo de este proyecto es el estudio de las herramientas y técnicas para detectar las amenazas y las vulnerabilidades que afectan a los Smartphones. Los sistemas operativos móviles que se estudiarán son Android e iOS.

Metodologías y estándares

A nivel mundial existen estándares relacionados con el análisis de vulnerabilidades, auditoría y pruebas de Intrusión que hemos seguido para la realización de este proyecto como son COBIT o ISACA.

Estructura del trabajo

En este punto describiremos los diferentes apartados que forman el proyecto y una breve descripción de cada uno. Lo apartados son:

1. Desarrollo del plan de trabajo
2. Metodología para el análisis de vulnerabilidades
3. Análisis de dispositivos móviles IOS
4. Análisis de dispositivos móviles Android
5. Escaneo de dispositivos móviles IOS
6. Evaluación y acceso al sistema en iOS
7. Escaneo de dispositivos móviles Android
8. Evaluación y acceso al sistema en Android OS
9. Informe final y conclusiones

Planificación temporal

En esta parte adjuntamos el diagrama de Gantt con las tareas a realizar y su planificación temporal, así como su duración y dependencia.

METODOLOGÍA PARA EL ANÁLISIS DE VULNERABILIDADES

Definición de análisis y auditoría de Smartphones

Una auditoría de seguridad informática sobre smartphones trata sobre la evaluación de los dispositivos móviles cuyo fin es detectar errores y fallos en el sistema, y que mediante un informe detallado se muestren los resultados verificados y las medidas y recomendaciones a tomar.

La metodología de análisis de vulnerabilidades informáticas, está enfocada a la protección total de los recursos que estén expuestos a posibles amenazas de seguridad informática.

Es un tipo de análisis que busca identificar e informar fallas en los dispositivos y en los procesos tecnológicos.

La metodología de análisis de vulnerabilidades y auditoría sobre smartphones ha sido estructurada en diferentes módulos.

Fases de la metodología

Llegado a este punto del desarrollo, hemos procedido a diseñar la metodología basándonos en los diferentes modelos existentes. Por tanto hemos conseguido desarrollar esta estructura modificando e incorporando nuevos elementos y valores que nos proporcionan una metodología nueva y consistente, y que a su vez nos permita aplicarla a la realidad, en cuanto a riesgos informáticos en entornos compuestos por smartphones.

El esquema con las diferentes fases es el siguiente:

Fase 1, Identificación: Esta fase consiste en la identificación y definición de los sistemas a auditar. El objetivo es la obtención de información sobre el dispositivo móvil.

Fase 2, Análisis: Análisis de los servicios de red en escucha o puertos activos, detección del sistema operativo y servicios inalámbricos en uso.

Fase 3, Acceso: Durante esta fase de procederá a identificar las vulnerabilidades del dispositivo y a explicar como podría realizarse su posterior explotación.

Fase 4, Resultados: En esta fase describiremos de manera simplificada los procesos realizados hasta llegar a obtener el objetivo, así como las técnicas utilizadas y las herramientas asociadas.

Fase 5, Informes: Esta es la última fase de la metodología, donde una vez obtenidos los resultados y verificados, se emite un informe indicando el establecimiento de las medidas preventivas de refuerzo y/o corrección a los problemas obtenidos.

Definición y análisis de amenazas de seguridad

En este apartado definimos el término "amenaza" en el ámbito de la seguridad informática. También enumeramos las amenazas existentes y hacemos una clasificación de estas.

Una amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, y en el caso de los Smartphones, sobre los elementos relacionados con la información y el propio dispositivo hardware.

Existen amenazas de diferentes tipos que generalmente se agrupan en criminales, físicas y negligentes. Las más comunes pertenecen al grupo de las criminales y a continuación enumeramos algunas, que son: Robo de información, Acceso a datos confidenciales, Infección por virus o malware y Ataques de phising.

Para entender los tipos de amenazas actuales, es necesario conocer el significado de malware, los tipos de malware existentes y cómo funcionan. El malware es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. Los más conocidos son: Virus, Ransomware, Troyanos y Spyware.

Las vías de acceso y contagio más comunes en los smartphones son a través de Vulnerabilidades, Ficheros descargados, navegación web, Aplicaciones fraudulentas, consecuencias de Root o Jailbreak y ataques de red.

ANÁLISIS DE DISPOSITIVOS MÓVILES IOS

Descripción y estructura del sistema operativo iOS

iOS es el nombre del sistema operativo desarrollado por la compañía Apple Inc. exclusivo para sus dispositivos. Este sistema operativo está optimizado para su hardware, lo que permite sacar el máximo rendimiento. El sistema operativo iOS posee una interfaz fluida, sencilla y elegante, sin mucha posibilidad de personalizar pero que ofrece una experiencia cómoda.

El kit de desarrollo de software(SDK) fue liberado el 6 de marzo de 2008, permitiendo así a los desarrolladores hacer aplicaciones para el iPhone.

El sistema operativo iOS deriva de macOS, que a su vez está basado en Darwin BSD, y por lo tanto es un sistema operativo tipo Unix. La arquitectura de iOS se basa en capas, las capas de nivel superior interactúan como intermediarias entre el hardware y las aplicaciones que se desarrollan.

Las capas de nivel superior se basan en las capas inferiores, proporcionan servicios y tecnologías más avanzadas para el desarrollo de aplicaciones, las capas inferiores poseen el control de los servicios básicos. iOS cuenta con cuatro capas de abstracción: la capa del núcleo del sistema operativo o “Core OS”, la capa de Servicios Principales o “Core Services”, la capa de Medios de comunicaciones o “Media” y la capa de"Cocoa Touch”.

Seguridad del sistema operativo iOS

En este punto del trabajo se describen los sistemas de seguridad que incorpora el sistema operativo iOS y el funcionamiento de estos sistemas. Se describen características como el Secure Boot Chain, la autorización en las actualizaciones OTA, el Secure Enclave, la encriptación y protección de datos del sistema, así como la firma de seguridad en las aplicaciones.

En el proyecto también se tratarán la seguridad de la red en iOS, así como los protocolos, sistemas y servicos de Internet. Algunos ejemplos son el TLS, VPN, Wi-fi, NFC, iMessage, iCloud, backups, Siri, etc.

Todos los dispositivos iOS combinan software, hardware y servicios que se han diseñado para funcionar conjuntamente con el fin de proporcionar la máxima seguridad y una experiencia de usuario transparente. iOS protege el dispositivo y los datos que contiene, así como el ecosistema en su totalidad, incluidas todas las acciones que los usuarios realizan de forma local, en redes y con servicios clave de Internet.

La seguridad del sistema se ha diseñado de modo que tanto el software como el hardware estén protegidos en todos los componentes centrales de los dispositivos iOS. Esto incluye el proceso de arranque, las actualizaciones de software y el coprocesador Secure Enclave.

ANÁLISIS DE DISPOSITIVOS MÓVILES ANDROID

Descripción y estructura del sistema operativo Android

Android es un sistema operativo orientado a dispositivos móviles, basado en una versión modificada del núcleo Linux. Inicialmente fue desarrollado por Android Inc., una pequeña empresa, que posteriormente fue comprada por Google.

La plataforma de hardware principal de Android es la arquitectura ARM, aunque también hay soporte para x86 en el proyecto Android-x86.

El sistema operativo Android es un sistema abierto, multitarea, que permite a los desarrolladores acceder a las funcionalidades principales del dispositivo mediante aplicaciones. Android depende de un Linux versión 2.6 para los servicios base del sistema como seguridad, gestión de memoria, gestión de procesos, stack de red, y modelo de drivers. El núcleo también actúa como una capa de abstracción entre el hardware y el resto del stack de software.

Android está formada por varias capas que facilitan al desarrollador la creación de aplicaciones. Además, esta distribución permite acceder a las capas más bajas mediante el uso de librerías, facilitando las tareas del desarrollador y así no precise programar a bajo nivel las funcionalidades necesarias para que una aplicación haga uso de los componentes de hardware del smartphone. Cada una de las capas utiliza elementos de la capa inferior para realizar sus funciones, es por ello que a este tipo de arquitectura se le conoce también como pila. La arquitectura de Android está formada por cinco capas, núcleo Linux, runtime de Android, Bibliotecas nativas, entorno de aplicación y Aplicaciones. Una de las características más importantes es que todas las capas están basadas en software libre.

Seguridad del sistema operativo Android

En esta parte del proyecto se describen los sistemas de seguridad que utiliza Android OS. Se tratan los sistemas de seguridad que implementa a nivel de sistema operativo, a nivel de núcleo, a nivel de capa de aplicaciones, el funcionamiento interno de particiones del sistema, permisos y cifrado de archivos, la gestión de memoria, actualizaciones del sistema, la seguridad a nivel de aplicaciones y procesos, etc.

Para proporcionar una buena seguridad a una plataforma de código abierto como Android, requiere de una robusta arquitectura de seguridad y de rigurosos programas de seguridad. Android fue diseñado con varias capas de seguridad que proporcionan la flexibilidad necesaria para una plataforma de carácter abierto como esta, mientras que proporcionan la protección para todos los usuarios de la plataforma. Los controles de seguridad fueron diseñados para reducir la carga de la misma sobre los desarrolladores.

Android pretende ser el sistema operativo más seguro y útil para plataformas móviles por proponer controles de seguridad de sistemas operativos tradicionales para:

- Proteger los datos del usuario.
- Proteger los recursos del sistema (incluyendo la conexión de red).
- Proporcionar el aislamiento de aplicaciones.

Para lograr estos objetivos, Android proporciona las siguientes características clave de seguridad:

- Una seguridad robusta a nivel de sistema operativo a través del núcleo de Linux.
- "Sandbox" de aplicación obligatorio para todas las aplicaciones.
- Seguridad en la comunicación entre procesos.
- Firma de aplicaciones.
- Permisos de aplicación y usuarios.

ESCANEO DE DISPOSITIVOS MÓVILES IOS

Exploración y análisis del dispositivo

En esta fase del proyecto, se pretende describir el procedimiento a seguir para lograr realizar la identificación del dispositivo y sistema a auditar. Con el fin de lograr obtener el máximo de información sobre el dispositivo móvil. En esta sección del proyecto se explica como identificar el dispositivo de forma visual y como hacerlo a través de su identificador IMEI, consultando en ambos casos la web del fabricante o la web de www.imei.info.

Realizando un escaneo a través de la red, siempre que el dispositivo esté conectado a esta, podremos identificar si este tiene hecho el Jailbreak. Con la información que iremos recopilando se podrá incluso conocer su versión de sistema operativo.

Llegado a este punto, después de haber explorado el dispositivo y analizado la información obtenida, debemos tener claro qué modelo de smartphone estamos estudiando, su versión de sistema operativo iOS y en el mejor de los casos, si el dispositivo tiene el Jailbreak hecho.

EVALUACIÓN Y ACCESO AL SISTEMA EN IOS

Identificación de vulnerabilidades y proceso de Jailbreak

En este apartado estudiamos el proceso de Jailbreak, como realizar Jailbreak a un dispositivo, las herramientas a utilizar y también donde consultar las vulnerabilidades públicas reportadas.

Para entender como se puede acceder a la totalidad de los datos de un smartphone, es necesario conocer el significado de Jailbreak, los tipos de Jailbreak existentes y cómo funcionan.

Este proceso permite al usuario disponer de control completo sobre el dispositivo móvil y acceder al mismo como “root”, o usuario privilegiado. El proceso de jailbreak se lleva a cabo a través de la explotación de vulnerabilidades en el hardware, iOS o alguna de las aplicaciones asociadas.

Las herramientas disponibles para realizar Jailbreak dependen de las diferentes versiones de iOS. La utilización de estos programas suele ser trivial, por lo que no se necesitan conocimientos técnicos avanzados para llevar a cabo el procedimiento.

Para poder conocer el nivel de seguridad y las posibles amenazas a las que está expuesto el dispositivo a analizar, debemos comprobar qué vulnerabilidades hay publicadas para la versión de iOS que tiene nuestro terminal. Para ello podremos consultar la web de CVE Details y la página oficial de soporte de Apple.

Métodos de explotación y acceso

En este apartado explicaremos como acceder a los datos de un dispositivo, los posibles casos que se pueden dar, las diferentes formas de acceder, así como las técnicas para saltarse u obtener el passcode de la pantalla de bloqueo.

Llegado a este punto podemos encontrarnos con diferentes casos:

1. Que para nuestro modelo y versión exista una herramienta de Jailbreak que no necesite el passcode.
2. Que nuestro dispositivo tenga el chipset A4 y por lo tanto es posible realizar el Jailbreak mediante el proceso BootRom.
3. Que no exista el Jailbreak para nuestro dispositivo.

En los 2 primeros casos, podremos conseguir hacer el Jailbreak y por lo tanto acceder a los datos, y en el caso 3 no podremos acceder. Solo podríamos intentar sacar el máximo de información del terminal mediante Siri, en el caso que esté activado, y realizando análisis del tráfico de red en el caso que estuviera conectado a alguna red Wifi.

Configuración del dispositivo y recomendaciones

En esta parte haremos un análisis de los controles de acceso y privacidad del sistema operativo iOS, así como de los servicios activos innecesarios y errores de configuración.

ESCANEO DE DISPOSITIVOS MÓVILES ANDROID

Exploración y análisis del dispositivo

En esta fase del proyecto, se pretende describir el procedimiento a seguir para lograr realizar la identificación del dispositivo y sistema a auditar. En esta sección del proyecto se explica como identificar el dispositivo a través de su identificador IMEI, consultando la web de www.imei.info

Debido a la gran cantidad de fabricantes que disponen de modelos de smartphones que utilizan Android como sistema operativo móvil, no es una tarea sencilla identificar de forma visual el modelo exacto de un terminal Android.

Es importante conocer el modelo de dispositivo porque esta es una información muy útil a la hora de rootear el terminal o firmware de forma manual. Ya que los archivos varían según el modelo del teléfono y debemos asegurarnos que la técnica a utilizar es la adecuada.

Android implementa diferentes métodos de bloqueo de seguridad, algunos mediante funciones genéricas para todos los dispositivos y otras solo disponibles en dispositivos con un hardware concreto. Explicamos algunas de ellas en este trabajo.

En esta fase del estudio, después de haber explorado el dispositivo y analizado la información obtenida, debemos tener claro qué modelo de smartphone estamos estudiando, su versión de sistema operativo Android y en el mejor de los casos, si el dispositivo tiene algún servicio en escucha que posteriormente nos sirva para explotar alguna vulnerabilidad.

EVALUACIÓN Y ACCESO AL SISTEMA EN ANDROID

Identificación de vulnerabilidades y Android rooting

En este apartado estudiamos el proceso de Rooteo, como realizar Root a un dispositivo, las herramientas a utilizar y también donde consultar las vulnerabilidades públicas reportadas.

Para entender como se puede acceder a la totalidad de los datos de un smartphone, es necesario conocer el significado de Rooteo, los tipos de Rooteo existentes y cómo funcionan.

El rooting o rooteo de dispositivos Android es el proceso que permite a los usuarios de teléfonos inteligentes con el sistema operativo móvil Android obtener control privilegiado. Esto significa ser un Superusuario y tener, por lo tanto, acceso total al sistema.

Para rootear o hacer root a un terminal existen diferentes métodos. El proceso para ser root depende del fabricante, del modelo de nuestro dispositivo y de la versión Android que está ejecutando.

En entornos Android tenemos diferentes tipos de rooteo, y no todos tienen las mismas implicaciones desde el punto de vista forense.

Como es necesario conocer un amplio abanico de métodos, técnicas y herramientas así como los criterios necesarios para poder evaluar la idoneidad de utilización de unas respecto a otras, en este proyecto solo presentaremos las más comunes.

En esta parte del proyecto vamos a conocer el nivel de seguridad y las posibles amenazas a las que está expuesto el dispositivo a analizar y qué vulnerabilidades hay publicadas que afecten al terminal.

Métodos de explotación y acceso

En esta sección vamos a explicar las diferentes formas que existen y que podría utilizar un atacante para acceder a un dispositivo Android. Explicaremos de forma breve las técnicas para evadir el código de bloqueo, como saber si tenemos acceso Root en un dispositivo, en que consiste en modo depuración USB, como acceder mediante ADB, etc. En primer lugar explicaremos qué metodologías y fases del proceso nos podemos encontrar a la hora de intentar adquirir los datos de un dispositivo móvil con Android. Para ello es necesario conocer un amplio abanico de métodos, técnicas y herramientas así como los criterios necesarios para poder evaluar la idoneidad de utilización de unas respecto a otras.

A la hora de seleccionar el método más adecuado, tenemos que tener en cuenta multitud de aspectos com o el tiempo del que disponemos, que información queremos extraer, el tipo de acceso que tenemos al dispositivo, y en concreto, cuál es la finalidad de acceder a al dispositivo, conseguir algún dato, tomar el control, realizar una auditoría o un análisis forense, etc.

Configuración del dispositivo y recomendaciones

En este apartado vamos a realizar un análisis de los controles de acceso y privacidad del sistema operativo Android, de los servicios activos innecesarios y el tratamiento de los errores de configuración. En primer lugar hablaremos de las actualizaciones, ya que son fundamentales porque en algunas ocasiones van a definir si el equipo es vulnerable o no.

ANÁLISIS DE DATOS

En este último apartado vamos a explicar el procedimiento a realizar para la extracción análisis de los datos, mediante la herramienta de análisis forense Oxygen Forensic Suite. Este procedimiento de análisis se podría realizar de forma manual, sin embargo el volumen de datos es tan grande que deberíamos pasar varias semanas con este proceso. Es por ello que para facilitar el trabajo haremos uso de Oxygen Forensic Suite, que nos permitirá analizar los datos de forma rápida y eficiente. Oxygen Forensic Suite es una herramienta comercial para el análisis forense en telefonía móvil. Es compatible con la mayoría de los teléfonos del mercado, aunque esta solución se especializa en la extracción y análisis de datos en smartphones, apoyándose en una interfaz cómoda e intuitiva.

En caso de querer analizar las aplicaciones de nuestro dispositivo para detectar el malware o simplemente realizar un análisis de los datos de forma rápida y cómoda, la herramienta seleccionada es Oxygen Forensic.

Y finalmente, otra de las características que pueden ser muy interesantes, es la posibilidad que nos ofrece esta herramienta de análisis forense para detectar aplicaciones spyware instaladas en el dispositivo,

procesando sus registros y archivos de configuración. La presencia de spyware en el teléfono puede significar que las actividades del usuario del teléfono fueron monitorizadas o controladas. Por supuesto, podremos generar diferentes informes de las evidencias obtenidas para su posterior exportación.

CONCLUSIONES

Para concluir con este trabajo explicamos como debería realizarse un análisis de seguridad sobre dispositivos con Android OS e iOS, y los principales aspectos que debemos tener en cuenta.

En el análisis de vulnerabilidades y la auditoria de seguridad en Smartphones no es sencillo establecer una metodología estricta a seguir. La realidad es que existe un gran número de modelos y marcas de smartphones, aunque la gran mayoría utilicen los sistemas operativos Android e iOS, con una gran cantidad de versiones y variantes, que a han ido surgiendo a lo largo de estos años.Esto tiene el inconveniente de que cada Investigador utilice técnicas y habilidades que se puede adquirir en base a la experiencia. Sin embargo, en este trabajo se pretende dar algunas pautas que pueden servir de guía para el analista que desea realizar un análisis sobre smartphones, concretamente sobre terminales con sistema operativo iOS y Android OS.

Para completar este proyecto sería recomendable la realización de varias pruebas de concepto en un laboratorio, con al menos dos dispositivos diferentes con los sistemas operativos iOS y Android OS respectivamente. Estas pruebas ayudarían a demostrar los procedimientos desarrollados en este trabajo y a dar a conocer el concepto práctico de las técnicas estudiadas.

ANEXO

En este apartado daremos algunas recomendaciones y medidas de prevención a tomar para garantizar que nuestros teléfonos e información están a salvo de ataques y no corren riesgo alguno.

También expondremos un plan de respuesta y mitigación en caso de infección por malware, de manera que puedan evitarse las infecciones o, en su defecto, que de presentarse sus consecuencias sean las mínimas aceptables.