TRABAJO FIN DE GRADO

GRADO EN INGENIERIA INFORMATICA

Android Shield

Detector de malware para Android

Autor
Nazaret Román Guerrero

Director
José Antonio Gómez Hernández

Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación

Granada, Junio de 2021

Android Shield
Detector de malware para Android

Nazaret Román Guerrero

Palabras clave: detector, malware, aplicación, permiso

Resumen

Desde que el sistema operativo de Android se lanzó al mercado en el año 2008, su uso ha crecido hasta alcanzar una cuota de mercado que superaba el 90% en el año 2018. Su amplio uso, tanto en dispositivos móviles como en tabletas, relojes inteligentes, televisores inteligentes (*SmartTV*) o, incluso, automóviles, ha propiciado también el desarrollo de malware o software malicioso.

Android cuenta con un amplio conjunto de aplicaciones (no nativas) y funcionalidades (nativas) en las distintas capas del sistema operativo para mantener el dispositivo seguro y a salvo de posibles ataques. Las aplicaciones intaladas, por lo general de una fuente segura y de confianza como la *Play Store*, pasan un control de seguridad (a través de una funcionalidad de Google llamada *Play Protect* que analiza la aplicación en busca de software maligno). Una vez instaladas en el dispositivo, todo depende del usuario.

Mantener el dispositivo y las aplicaciones actualizadas y acceder solo a sitios seguros son medidas básicas de seguridad, como también lo es la gestión de permisos. Android cuenta con un amplio conjunto de permisos que controlan el acceso a las distintas partes del dispositivo y las acciones que puede realizar cada aplicación. El sistema de permisos es eficaz para evitar ataques siempre y cuando el usuario no conceda acceso libre a aplicaciones que no deberían solicitar ciertos permisos considerados peligrosos.

Siguiendo esta línea de acción, se ha desarrollado una aplicación para Android que detecte los permisos de cada aplicación y, según los permisos peligrosos solicitados, la clasifique en una aplicación benigna o maligna. Para llevar a cabo esta actividad, se utiliza un modelo entrenado mediante los permisos extraídos de distintas muestras de aplicaciones, tanto benignas como malignas, alcanzando un ratio de acierto del 99%.

Android Shield: An Android malware detector

Nazaret Román Guerrero

Keywords: detector, malware, application, permission

Abstract

Since the Android OS was launched on the market in 2008, its use has grown to reach a market share that exceeded 90% in 2018. Its wide use, both in mobile devices and tablets, smartwatches, smart TVs or even cars, has also led to the development of malware or malicious software.

Android has a wide set of non-native applications and native functionalities in the different layers of the OS to keep the device safe and sound from possible attacks. Installed apps, usually from a trusted source like the *Play Store*, pass a security check (through a Google feature called *Play Protect* that scans the app for malicious software). Once the software is installed on the device, it all depends on the user.

Keeping the device and applications up-to-date and accessing only secure sites are basic security measures, as it is managing permissions. Android has a wide set of permissions that control the access to the different parts of the hardware, and also the actions that each application can perform. The permission system is effective in preventing attacks as long as the user does not grant free access to applications that should not request certain permissions considered dangerous.

Following this line of action, we have developed an Android application that detects the permissions of each application and, according to the dangerous permissions requested, classifies it into a benign or a malicious application. To carry out this activity, a model trained by sets of permissions extracted from different samples of applications, both benign apps and malware, has been used, reaching a success rate of 99%.

D. **José Antonio Gómez Hernández**, Profesor del Área de XXXX del Departamento de Lenguajes y Sistemas Informáticos de la Universidad de Granada.

Informa:

Que el presente trabajo, titulado ***Android Shield, Detector de malware para Android***, ha sido realizado bajo su supervisión por **Nazaret Román Guerrero**, y autorizamos la defensa de dicho trabajo ante el tribunal que corresponda.

Y para que conste, expiden y firman el presente informe en Granada a X de junio de 2021 .

El director:

José Antonio Gómez Hernández

Agradecimientos

Índice general

Capítulo 1

Introducción

1.1. Un poco de historia

Desde que se lanzó en el año 2008 de la mano de la empresa taiwanesa HTC, el sistema operativo **Android**, desarrollado por Android Inc. y más tarde adquirido por Google, ha extendido su uso alrededor de todo el mundo y actualmente cuenta con no menos de 3000 millones de dispositivos que dependen directamente de él, superando con creces su principal competidor iOS, de Apple.

Basado en núcleo de Linux, el código fuente de Android es *Open Source* (conocido como *Android Open Source Project* o *AOSP*) y está licenciado bajo la Licencia Apache.

En 2005, Google compró Android Inc. y dos años más tarde, en 2007, se creó la *Open Handset Alliance*, un conjunto de fabricantes y desarrolladores de hardware, software y operadores de servicio que, junto a Google, lanzaron al mercado la primera versión del sistema operativo (Android 1.0: Apple Pie). No obstante, no fue hasta 2008 cuando apareció el primer teléfono inteligente, el HTC Dream, que utilizaba este sistema operativo.

Desde ese momento, el sistema operativo fue creciendo y desarrollándose cada vez más hasta alcanzar la versión actual, Android 11.

1.2. Uso del sistema operativo Android

Los dispositivos tecnológicos portables, en concreto los teléfonos inteligentes, se han convertido en un pilar fundamental de nuestra vida. A través de estos dispositivos somos capaces de buscar información, mantener el contacto con gente de alrededor de todo el mundo a través de llamadas de teléfono o mensajería instantánea e incluso hacer compras por Internet. Esto ha supuesto un gran avance en materia de comunicaciones y desarrollo de software, pero también ha potenciado el desarrollo de software malicioso, maligno o malware que pone en

peligro la seguridad de nuestros datos personales como la localización, los datos bancarios o la información de contacto.

Android es un sistema con una arquitectura por capas que aisla unas partes del dispositivo de otras y facilita la abstracción en cuanto a programación de aplicaciones. Esto dificulta los ataques en gran medida, pero a pesar de ser robusto, el sistema operativo puede contener agujeros de seguridad que los atacantes pueden utilizar. Su frecuencia de actualización recomendada es mensual, publicandose parches de seguridad de manera continuada para cubrir las vulnerabilidades encontradas y mantener el dispositivo, y por tanto, los datos, a salvo.

A pesar de ello, los atacantes aprovechan los puntos débiles y las vulnerabilidades del día cero (*zero-day vulnerabilities*) para acceder a los dispositivos de una forma u otra y extraer información, por lo general con objetivos económicos.

Entre las medidas de seguridad con las que cuenta Android, destaca su amplio conjunto de permisos. El acceso a las distintas partes del dispositivo, las acciones que se pueden realizar sobre los datos o la recogida y eliminación de información están estrictamente controladas por este sistema. Dentro del conjunto de permisos hay algunos considerados peligrosos o arriesgados (*risky permissions*). Mediante el control riguroso de estos permisos, el sistema de seguridad de Android se ve reforzado y es eficaz para detener posibles amenazas... siempre y cuando el usuario sea consciente de los permisos que da a las distintas aplicaciones.

Es aquí donde los atacantes pueden sacar provecho de las vulnerabilidades del sistema. Si un usuario descarga una aplicación de una fuente no segura y concede ciertos permisos sin detenerse a pensar qué uso hará la aplicación con la información contenida en su sistema, los atacantes podrán acceder a todas aquellas partes del dispositivo que deseen, extraer toda la información que quieran, hacer llamadas de teléfono, enviar mensajes SMS o recolectar información sobre los contactos del usuario.

1.3. Objetivo de este proyecto

La idea principal de este proyecto es crear una aplicación que ayude a mejorar la seguridad del dispositivo Android haciendo una clasificación de las demás aplicaciones instaladas en aplicaciones benignas o malware. Para ello, utilizando los permisos declarados en el MANIFEST.XML, se ha entrenado un modelo que clasifique dichas aplicaciones y muestre la estimación hecha para que el usuario sepa si su sistema es vulnerable a amenazas causadas por malware camuflado en forma de aplicación.

poniendo de manifiesto qué
fff
fff
ff

ff
ff
ff
ff

Capítulo 2

Descripción del problema

Capítulo 3

Estado del arte

El software libre y sus licencias [?] ha permitido llevar a cabo una expansión del aprendizaje de la informática sin precedentes.

Capítulo 4

Planificación

4.1. Metodología utilizada

4.2. Temporización

4.3. Seguimiento del desarrollo

Capítulo 5

Análisis del problema

Capítulo 6

Implementación

La implementación del software se ha dividido en hitos. Estos, han sido definidos en Github y cada uno de ellos contiene un grupo de *issues* que se corresponden con las distintas mejoras que se han ido incorporando al software a lo largo de su desarrollo.

Capítulo 7

Conclusiones y trabajos futuros