PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

EVALUACIÓN DE TECNOLOGÍAS, HERRAMIENTAS Y PROTOCOLOS CON APLICACIONES ANTI-ROBO PARA EL RASTREO DE DISPOSITIVOS MÓVILES

CARLOS RICARDO POZO VINTIMILLA

DIRECTOR: ING. ANDRÉS JIMÉNEZ PACHECO

QUITO, JULIO 2018

1. Contenido

Índice de ilustraciones

Índice de tablas

INFORMACIÓN DEL PROYECTO

1. Tema

Evaluación de tecnologías, herramientas y protocolos con aplicaciones anti-robo para el rastreo de dispositivos móviles.

2. Justificación

La investigación del presente proyecto ayudará a entender los protocolos y herramientas informáticas que se utilizan en aplicaciones que rastrean móviles robados, tomando como caso de estudio distintas aplicaciones anti-robo como Prey y Open Source[1]Theft Recovery. Se considerarán temas como mapas de geolocalización, Global Positioning System (GPS)[2] y Global System for Mobile Communications (GSM)[3], potencia de señal y precisión, coordenadas de precisión, información de usuarios y dispositivo, captura de pantalla silenciosa, uso de cámaras frontales y posteriores del móvil, control zones, etc., temas que serán estudiados(Prey, 2018).

Este trabajo aportará conocimientos al desarrollo de aplicaciones móviles anti-robo y proporcionará al usuario conocimientos sobre distintas tecnologías y funcionalidades de los dispositivos móviles Android[4], con lo cual se estaría apoyando a la sociedad con ventajas tecnológicas de herramientas de análisis y protección informática, que se puede aprovechar para contrarrestar la constante inseguridad de la información y disminuir el hurto de dispositivos inteligentes.

3. Planteamiento del problema

En marzo de 2016, Crime Survey para Inglaterra y Gales (CSEW) sugirió que el 81% de los adultos tenían un teléfono móvil (más de 46 millones de personas), igual porcentaje se registró el año 2017.El estudio de campo del año 2016, realizado por Focus on Property Crime, sugiere

[1] Open Source: Se refiere a código abierto y es un modelo de desarrollo de software basado en la colaboración abierta

[2] Sistema de Posicionamiento Global: Se refiere a un sistema que permite determinar en toda la Tierra la posición de un objeto

[3] Sistema global para las comunicaciones móviles: Es el sistema global para las comunicaciones móviles

[4] Android: Es un sistema operativo basado en el núcleo de linux

que el 1%de los propietarios de teléfonos móviles, equivalente a 446.000 personas, tuvieron un robo en el año anterior (Focus on property crime: year ending March, 2016). Para el año 2020, en América Latina y el Caribe se estima que se incrementarán nuevos suscriptores de internet móvil en alrededor de 150 millones (Asociación GSM, 2016); esto indica que millones de personas guardarán información confidencial en cada uno de estos dispositivos. Llamadas registradas, números telefónicos, número y duración de llamadas, mensajes registrados, frecuencia de revisión de un correo electrónico, historial es de acceso a internet, ubicación geográfica, imágenes, videos, información sensible, pueden ser vulnerados(Privacy in the Age of the Smartphone, 2017;PrivacyRightsClearingHouse, 2017).

La información privada de los dispositivos es tan relevante, que empresas de todo tipo compran información privada para monitorear y rastrear a los usuarios con diferentes propósitos. Las últimas revelaciones sobre las potentes herramientas de hackeo del gobierno de los Estados Unidos alertan que el espionaje alcanza a los hogares y billones de usuarios en todo el mundo, mostrando como una notable variedad de dispositivos cotidianos pueden ser intervenidos para espiar a sus dueños (The Washington Post, 2017).

En la actualidad existen aplicaciones en el mercado que ofrecen rastreo de sistemas y aplicaciones anti-robo para detectar el uso no autorizado de tarjetas Subscriber Identity Module (SIM)[5]. La mayoría de estas aplicaciones proveen soluciones delicadas utilizando métodos de rastreo que monitorean el dispositivo. Sin embargo, si solo se habilita el dispositivo móvil con el sistema GPS integrado para recuperar la información, sería insuficiente para rastrear el teléfono inteligente (Abirami, Anantha, Annapoorani & Padma, 2014).

Las aplicaciones inteligentes anti-robo de Android, como Cerberus Anti Theft, han intentado mejorar la seguridad de los dispositivos móviles integrando herramientas de ciberseguridad y protocolos de difícil rastreo y anulación para el criminal (Cerberus Anti Theft–Officia lWebsite, 2017). A muchas compañías y gobiernos no les interesa que el público entienda cómo funcionan estas aplicaciones, ya que afectaría sus ingresos o políticas, por lo cual la mayoría no tiene su código abierto, limitando el progreso de nuevas ideas y funcionalidades(Simon& Anderson, 2015).

La arquitectura del dispositivo Android es muy versátil y tiene una vasta cantidad de librerías, herramientas y APIs; sin embargo, para los desarrolladores la empresa Google facilita la

[5] SIM: Es una tarjeta inteligente desmontable usada en teléfonos móviles. Almacena de forma segura la clave de servicio del suscriptor usada para identificarse ante la red

documentación de funcionalidades específicas para otras aplicaciones anti-robo que no sean de su propiedad, como lo es FindMyDevice de Google. Existe la limitación y la restricción impuesta por las APIs y la arquitectura de Android por parte de Google (Simon & Anderson, 2015).

La ineficiencia en las aplicaciones anti-robo es muy amplia pues existen muchas opciones que están desactualizadas, no consideran las últimas tendencias tecnológicas, protocolos ni herramientas. También existe una amplia variedad de opciones que en la práctica no logran cumplir las expectativas del usuario.

Por otro lado, muchas personas no tienen conocimiento sobre la existencia de aplicaciones anti-robo y la seguridad que proporcionan a los dispositivos. En el mercado hay muchas opciones y los usuarios no pueden distinguir entre tantas funcionalidades y aplicaciones.

Este trabajo de titulación propone realizar un análisis con diferentes herramientas informáticas forenses de los protocolos de distintas aplicaciones anti-robo en dispositivos Android como Prey: Open Source Theft Recovery y las herramientas y tecnologías que componen los mismos.

4. Objetivos

Objetivo General

Evaluar tecnologías, herramientas y protocolos que utilizan distintas aplicaciones anti-robo para el rastreo de dispositivos móviles.

Objetivos Específicos

Entender la arquitectura interna del teléfono inteligente con sistema operativo Android.

Identificar distintos protocolos y características que utilizan aplicaciones anti-robo mediante herramientas de análisis forense.

Comparar entre las diferentes aplicaciones anti-robo para el rastreo de dispositivos móviles open source y privadas.

Evaluar funcionalidades utilizadas en combinación con hardware y software del dispositivo Android en aplicaciones anti-robo.

1. Capítulo I: Arquitectura interna del dispositivo inteligente con sistema operativo Android

En el presente acápite se revisará la arquitectura interna del sistema operativo Android para teléfonos inteligentes. Se repasará su arquitectura, aplicaciones, componentes.

1.1. Arquitectura de hardware

Los teléfonos inteligentes nos proporcionan la capacidad de una computadora estándar y brindan absoluta[a.1] movilidad y portabilidad. Sin embargo, la arquitectura de un teléfono inteligente es significativamente diferente, comparada con las arquitecturas de hardware convencionales. Las múltiples unidades de cómputo que son la parte más obvia de la Central Processing Unit(CPU)[6]convencional no pueden caber en un teléfono inteligente ya que demandan[a.2] mucha energía. Por lo tanto, es necesario realizar muchos cambios en el diseño y la arquitectura de la CPU convencional para que los procesadores sean aptos en teléfonos inteligentes o cualquier otro dispositivo ultra portátil (Kuma, Pawar&Aggarwal, 2014).

Uno de los grandes problemas es que más características, significan más chips y más ciclos de procesamiento, lo que implica mayor consumo de energía. Debido a que las baterías no evolucionan a la misma velocidad que el apetito de los fabricantes y compradores, siempre existe una compensación entre la batería y el dispositivo móvil.

1.1.1.ARM

Según Chuang (2010) la arquitectura Advanced RISC Architecture(ARM)[7]solucionó [a.3]las restricciones debido a su bajo consumo de energía y un rendimiento razonable, sus características se detallan a continuación:

- Procesador de menor tamaño para ahorrar el consumo de energía.
- Alta densidad de código para memoria limitada y restricciones físicas de tamaño.
- Habilidad de utilizar memoria lenta y de bajo costo.

[6] Unidad central de procesamiento: Hardware que interpreta las instrucciones de un programa informático mediante la realización de las operaciones básicas

[7]Advanced RISC Architecture: Es una arquitectura RISC (Ordenador con Conjunto Reducido de Instrucciones) de 32bits

- Tamaño de matriz reducido para reducir el costo de fabricación y acomodar más periféricos.

Una ventaja es la integración de componentes y el uso de controladores dedicados para diferentes funciones, donde casi todo lo hace el procesador principal. La ventaja de usar controladores dedicados es que realizan sus funciones directamente en hardware, en lugar de implementación de software y tienen una ejecución muy rápida. Por lo tanto, pueden realizar sus tareas con menos transistores y menos ciclos de procesamiento, lo que se traduce en un menor consumo de energía. Cualquier teléfono inteligente tiene varios de estos controladores, que están apagados la mayor parte del tiempo, y están despiertos solo cuando tienen trabajo que hacer. Esta arquitectura requiere menos circuitos comparados con la arquitectura X86 de una PC (Kuma, Pawar & Aggarwal, 2014).

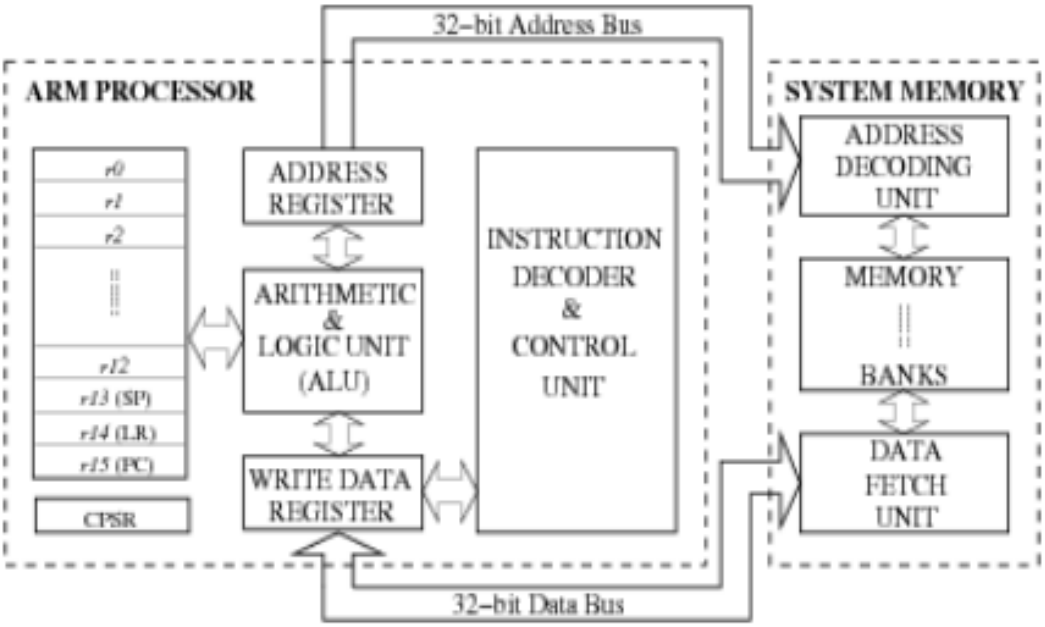

Ilustración1: ARM Processor Architecture (Kuma, Pawar & Aggarwal, 2014)

Chuang (2010) describe la arquitectura ARM con cuatro reglas principales de diseño:

- Instrucciones: conjunto reducido / ciclo único / longitud fija
- Pipeline: decodificar en una etapa / sin necesidad de microcódigo
- Registros: un gran conjunto de registros de uso general
- Cargar / almacenar arquitectura: las instrucciones de procesamiento de datos se aplican a registrar; cargar / almacenar para transferir datos desde la memoria.

1.1.1.1. Set de registros

El Manual de Referencia de Arquitectura ARM, 2005, especifica que tiene 31 registros de 32 bits de propósito general. En cualquier momento, 16 de estos registros son visibles. Los otros registros se utilizan para acelerar el procesamiento de excepciones. Todos los especificadores de registro en las instrucciones ARM pueden abordar cualquiera de los 16 registros visibles.

El banco principal de 16 registros es utilizado por todos los códigos no privilegiados. Estos son los registros de modo de usuario. El modo de usuario es diferente de todos los demás modos, ya que no tiene privilegios, lo que significa que:

- El modo de usuario solo puede cambiar a otro modo de procesador generando una excepción. La Instrucción Software Interrupt (SWI[ED4]) proporciona esta facilidad desde el control del programa
- Los sistemas de memoria y los coprocesadores pueden permitir que el modo de usuario tenga menos acceso a la memoria y la funcionalidad del coprocesador que a un modo privilegiado

La arquitectura ARM tiene siete modos para operar, así lo determina el Centro de Información de ARM (2018), estos son:

- El modo de usuario es el estado habitual de ejecución del programa ARM y se utiliza para ejecutar la mayoría de los programas de aplicación.
- El modo de Interrupción Rápida (FIQ) admite una transferencia de datos o un proceso de canal.
- El modo de Interrupción (IRQ) se utiliza para el manejo de interrupciones de propósito general.
- El modo Supervisor (SVC) es un modo protegido para el sistema operativo.
- El modo Abortar (ABT) se ingresa después de un dato o instrucción Prefetch Abort.
- El modo del Sistema (SYS) es un modo de usuario privilegiado para el sistema operativo.

1.1.1.2. Ejecución de instrucciones

Una instrucción que procesa datos requiere de dos operandos, uno de ellos siempre es un registro y el otro es un segundo registro o un valor inmediato. El segundo operando pasa a través del registro de desplazamiento Barrel Shifter, donde sufre un desplazamiento, luego se

combina con el primer operando en la Unidad Aritmética Lógica(ALU)[8]. Finalmente, el resultado de la ALU se escribe en el registro destino y se puede actualizar el registro de código de condición. Todas estas instrucciones tienen lugar en un único ciclo de reloj(Canel, 2007).

La técnica pipeline aprovecha un método para optimizar los recursos de hardware y también el rendimiento del procesador. Consiste en comenzar a procesar una instrucción antes de que se haya finalizado de procesar la actual (Canel, 2007[ED5]).

El proceso del pipeline(ARM Architecture Overview, n.d.) se determina de la siguiente manera:

- Se extrae la instrucción de la memoria
- Decodificación de registros utilizados en instrucción
- Registro(s) leído(s) desde el Banco deRegistro y operación de ALU escribe registro(s) de nuevo en el Banco del Registro

1.1.1.3. Carga y almacenamiento

La arquitectura ARM admite dos amplios tipos de instrucciones que cargan o almacenan el valor de un solo registro, o un par de registros, desde o hacia la memoria:

- El primer tipo puede cargar o almacenar una palabra de 32 bits o una de 8 bits sin firmar byte.
- El segundo tipo puede cargar o almacenar una media palabra sin firmar de 16 bits, y puede cargar y firmar para extender una media palabra de 16 bits o un byte de 8 bits(ARM Architecture Reference Manual, 2005).

El set de instrucciones solamente procesará (adición, substracción, etc.) valores que estén en los registros o directamente especificados dentro de la instrucción en sí misma y siempre se obtendrá el resultado de tales procesos en un registro. Las únicas operaciones que se aplican a la memoria son aquellas que copian datos de la memoria en los registros (instrucciones de carga) o copian datos de los registros en la memoria (instrucciones de almacenamiento). ARM no soporta operaciones memoria a memoria(Canel, 2007).

1.1.1.4. Sistema de memoria

[8] Unidad Aritmética Lógica: Es un circuito digital que calcula operaciones aritméticas y operaciones lógicas entre valore de los argumentos

Los requisitos del sistema de memoria de estas aplicaciones varían considerablemente, desde simples bloques de memoria con un mapa de direcciones planas, hasta sistemas que utilizan alguno o todos los siguientes para optimizar el uso de recursos de memoria: Múltiples tipos de memoria, Cachés[9], Búferes[10]de escritura, Memoria Virtual y otras técnicas de reasignación de memoria (ARM Architecture Reference Manual, 2005).

ARM tiene un estado de memoria. La memoria se puede ver como un arreglo lineal de bytes numerados desde el cero hasta el 2^{32} -1. Los datos pueden ser bytes (8 bits), de medias palabras (16 bits) o palabras (32 bits). Las palabras están siempre alineadas en bandas de 4 bytes y las medias palabras están alineadas en bandas de bytes pares (Canel, 2007).

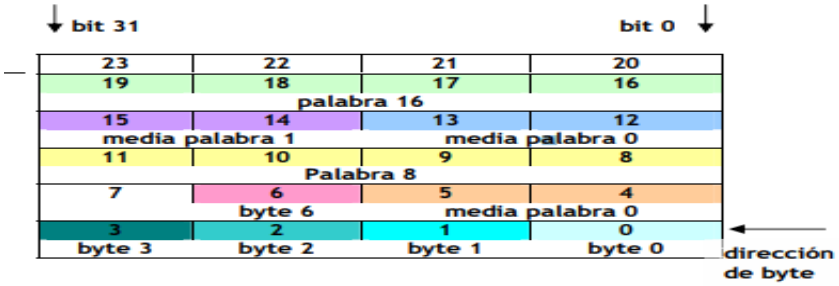

Ilustración 2: Organización de la memoria ARM (Canel, 2007)

Podemos concluir que ARM es la arquitectura que se debe utilizar para teléfonos inteligentes o cualquier otro teléfono con características similares. ARM deriva sus raíces de la arquitectura de computadora RISC ofreciendo simplicidad al estar compuesto por muy pocas instrucciones de acceso a la memoria.

1.1.1.5. Procesadores CPU

Los diferentes dispositivos portátiles con Android incorporan diferentes CPU que, a su vez, admiten diferentes conjuntos de instrucciones. Cada combinación de CPU y conjuntos de instrucciones tiene su propia Interfaz Binaria de Aplicación (ABI). La ABI define con gran precisión la manera en que el código máquina de una aplicación debe interactuar con el sistema durante el tiempo de ejecución. Se debe especificar una ABI para cada arquitectura de

[9] Memoria Cache: Es un tipo de memoria volátil. Su función es almacenar instrucciones y datos a los que el procesador debe acceder continuamente

[10] Búfer de Datos: Es un espacio de memoria, en el que se almacenan datos de manera temporal

CPU con se desea que funcione la aplicación(Administración de ABI | Android Developers, 2018).

Tabla 1: ABI y Notas

ABI	Notas
armeabi	Sin cálculo de punto flotante asistido por hardware.
armeabi-v7a	Incompatible con dispositivos ARMv5, v6.
arm64-v8a	
x86	Incompatible con MOVBE o SSE4.
x86_64	
mips	Usa cálculo de punto flotante asistido por hardware y supone una relación de reloj CPU: FPU de 2:1 para obtener la máxima compatibilidad. No proporciona micromips ni MIPS16.
mips64	

(Administración de ABI | Android Developers, 2018)

1.2. Arquitectura de Software

Android es un sistema operativo y una plataforma de programación desarrollada por Google para dispositivos inteligentes y otros dispositivos móviles (tablets). Puede correr en diferentes dispositivos de diferentes fabricantes. Android incluye un Software Development Kit (SDK)[11] para escribir código original y ensamblar módulos de software para crear aplicaciones Android. También cuenta con un Marketplace [12]llamado Google Play.

Para el desarrollo eficiente de aplicaciones Google ofrece un Integrated Development Environment(IDE)[13], en Java es llamado Android Studio, con características avanzadas para desarrollo, depuración y empaquetado en aplicaciones Android.

Android provee una arquitectura abundante de desarrollo(Training, 2017). Es un entorno operativo completo que se basa en el kernel de Linux, la arquitectura del sistema Android está compuesto por diferentes capas. El sistema operativo Android es una pila de componentes de software que se divide aproximadamente en cinco secciones y cuatro capas

[11] Kit de desarrollo de software: Conjunto de herramientas de desarrollo de software que le permite al programador crear una aplicación informática para un sistema concreto

[12] Marketplace: Son plataformas online creadas por una empresa que actúa como un tercero neutral para poner en contacto a compradores y vendedores

[13] Entorno de desarrollo integrado: Es una aplicación informática que proporciona servicios integrales para facilitarle al programador el desarrollo de software

principales(Shaheen, Asghar & Huss, 2017). Esto se muestra a continuación en el diagrama de la arquitectura.

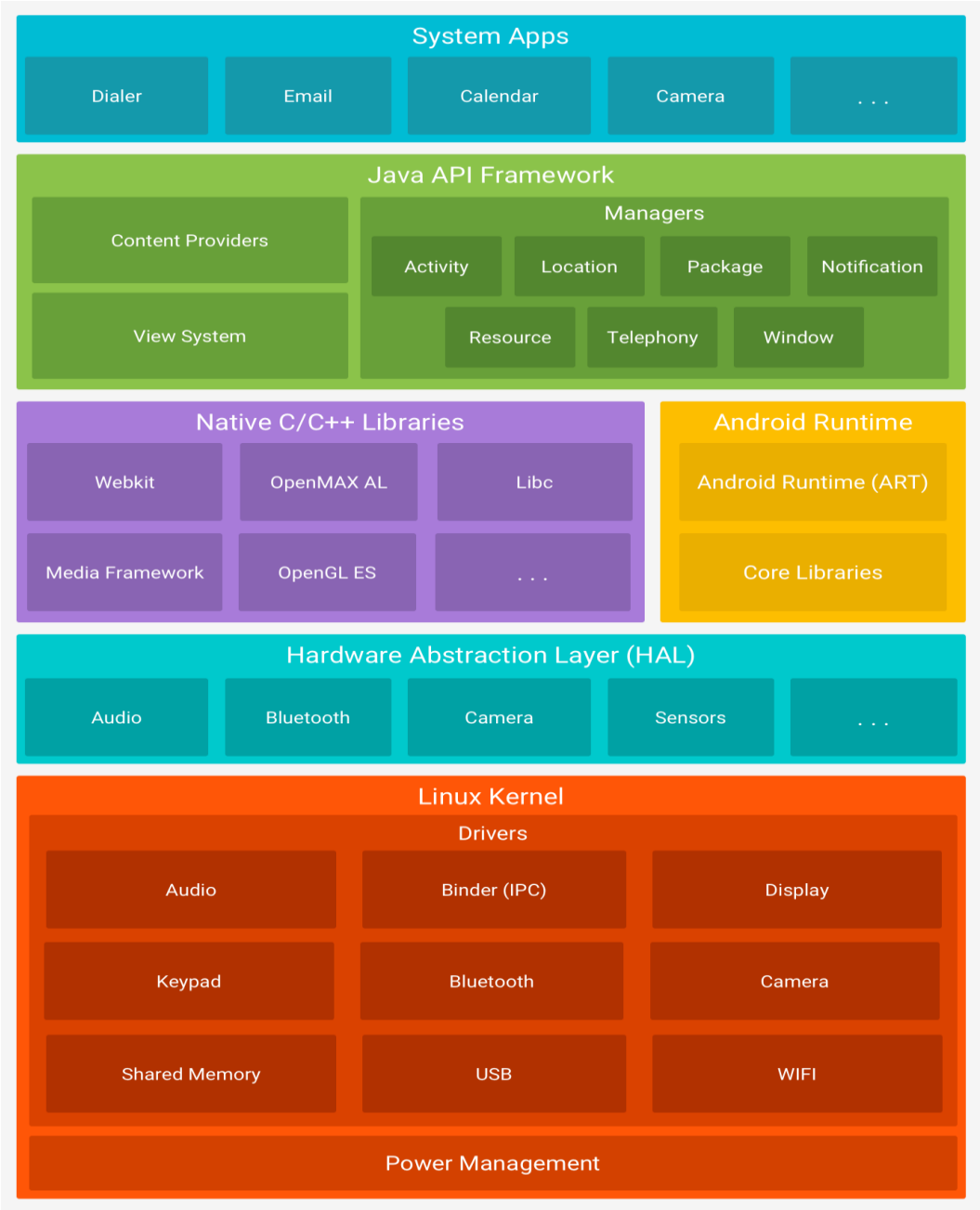

Ilustración 3: Pila de software de Android (Arquitectura de la plataforma | Android Developers, 2018

1.3.1.Aplicaciones del Sistema

Todas las aplicaciones de Android, esto incluye un navegador, alarma, calculadora, calendario, cámara, reloj, contactos, marcador, correo electrónico, reproductor multimedia, álbum de

fotos, SMS/MMS[14]y marcación por voz y otros, están escritas usando el lenguaje de programación Java(Shaheen, Asghar & Huss, 2017).

Las aplicaciones incluidas en la plataforma no tienen un estado especial entre las aplicaciones que el usuario elige[a.6] instalar; por ello, una aplicación externa se puede convertir en el navegador web, el sistema de mensajería Servicio de Mensajes Cortos (SMS), o incluso, el teclado predeterminado del usuario (existen algunas excepciones, como la aplicación de configuración del sistema). Estas aplicaciones permiten a los desarrolladores reutilizar funcionalidades de aplicaciones del sistema ya existentes (Arquitectura de la plataforma | Android Developers, 2018).

La capa Java API Framework brinda las funcionalidades requeridas a la capa de aplicaciones(New Tracking Rootkit at Application Layer in Android, 2017).

1.3.2.Java API Framework

Esta capa es utilizada con mayor frecuencia por desarrolladores de aplicaciones. Android ofrece a los desarrolladores la capacidad de crear diversas aplicaciones con un desarrollo abierto. Los desarrolladores tienen acceso completo a las mismas Application Programming Interface (API)[15]del Framework[16]utilizadas por las aplicaciones centrales. La arquitectura de la aplicación está diseñada para simplificar la reutilización de componentes; cualquier aplicación puede publicar sus capacidades y cualquier otra aplicación puede hacer uso de esas capacidades (Mohmedhussen & Altaee, 2017).

El Framework de aplicaciones Android incluye:

- Un conjunto de vistas completo y extensible que se utiliza para crear una aplicación con interfaz gráfica. Las vistas pueden estar constituida por listas, cuadrículas, cuadros de texto, botones e incluso un navegador web embebido

[14] Servicio de mensajería multimedia: Es un estándar de mensajería que le permite a los teléfonos móviles enviar y recibir contenidos multimedia, incorporando sonido, video o fotos.

[15] Interfaz de programación de aplicaciones: Es un conjunto de subrutinas, funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción

[16] Framework: Es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar

- Un conjunto de proveedores de contenido que permiten a las aplicaciones acceder a los datos de otras (como contactos) o compartir sus propios datos

- Un administrador de recursos responsable proporciona acceso a recursos no esenciales, como cadenas localizadas, gráficos y archivos de diseño

- Un administrador de notificaciones responsable de habilitar todas las aplicaciones para mostrar alertas personalizadas en la barra de estado

- Un administrador de actividades es responsable de administrar el ciclo de vida de las aplicaciones y proporciona una pila de navegación común

- El gerente de ubicaciones responsable de activar alertas cuando el usuario ingresa o sale de una ubicación geográfica específica

- El Administrador de paquetes es responsable de recuperar los datos sobre los paquetes instalados en el dispositivo

- El administrador de ventanas es el responsable de crear vistas y diseños

- El gerente de telefonía es el responsable de manejar la configuración de la conexión de red y toda la información sobre los servicios en el dispositivo (Shaheen, Asghar & Huss, 2017)

1.3.3.Librerías

Android tiene un conjunto de bibliotecas C / C ++ utilizadas por varios componentes del sistema Android. Estas bibliotecas están expuestas a los desarrolladores. La biblioteca del sistema C es una implementación derivada de Berkeley Software Distribution(BSD) del estándar(Mohmedhussen & Altaee, 2017).

Muchos componentes y servicios centrales del sistema Android, como el Android RunTime(ART) y la Hardware Abstraction Layer(HAL), se basan en código nativo que requiere bibliotecas nativas escritas en C y C++. La plataforma Android proporciona la API del Framework de Java para exponer la funcionalidad de algunas de estas bibliotecas nativas a las

apps. Por ejemplo, puedes acceder a Open Graphics Library (OpenGL ES) a través de la Java OpenGL API del Framework de Android para agregar a tu App compatibilidad con los dibujos y la manipulación de gráficos 2D y 3D. Si desarrollas una App que requiere C o C++, puedes usar el NDK de Android para acceder a algunas de estas bibliotecas de plataformas nativas directamente desde tu código nativo (Arquitectura de la plataforma | Android Developers, 2018).

GNU Libs (glibc) es demasiado grande y complicado para teléfonos móviles, por lo que Android implementa su propia versión especial de libc, Bioniclibc, que tiene un tamaño más pequeño de 200K. Algunas de las características eliminan algunas funciones complicadas de C ++, la más importante (Shaheen, Asghar & Huss, 2017) Android Runtime

Para los dispositivos con Android 5.0 (nivel de API 21) o versiones posteriores, cada App ejecuta sus propios procesos con sus propias instancias del tiempo de ejecución de Android (ART). El ART está escrito para ejecutar varias máquinas virtuales en dispositivos de memoria baja ejecutando archivos DEX, un formato de código de bytes diseñado especialmente para Android y optimizado para ocupar un espacio de memoria mínimo. Crea cadenas de herramientas, como Jack, y compila fuentes de Java en código de bytes DEX que se pueden ejecutar en la plataforma Android (Arquitectura de la plataforma | Android Developers, 2018).

Runtime incluye bibliotecas principales y la máquina virtual Dalvik. Las bibliotecas principales tienen un conjunto de bibliotecas centrales que proporciona la mayor parte de la funcionalidad disponible en las bibliotecas centrales de la programación Java (Mohmedhussen & Altaee, 2017).

Antes de Android 50 (nivel de API 21), Dalvik era el tiempo de ejecución del sistema operativo. Si la App se ejecuta en ART, también debe funcionar en Dalvik, pero es posible que no suceda lo contrario(Arquitectura de la plataforma | Android Developers, 2018).

1.3.4.Capa de abstracción de hardware (HAL)

La HAL brinda interfaces estándares que exponen las capacidades de hardware del dispositivo al Framework de la Java API de nivel más alto. La HAL consiste en varios módulos de biblioteca y cada uno de estos implementa una interfaz para un tipo específico de componente de

hardware, como el módulo de la cámara o de bluetooth[17]. Cuando el Framework de una API realiza una llamada para acceder a hardware del dispositivo, el sistema Android carga el módulo de biblioteca para el componente de hardware en cuestión(Arquitectura de la plataforma | Android Developers, 2018).

HAL separa las preocupaciones en la arquitectura del sistema Android, ya que desacopla el software y la capa del Framework del sistema operativo. Esto produce que las aplicaciones no se rompan cuando el hardware es modificado (Schmidt, 2017).

1.3. Kernel de Linux

La base de la plataforma Android es el kernel de Linux. Es compatible con los servicios básicos del sistema, como la seguridad, la gestión de memoria, la gestión de procesos, la pila de red y el modelo de controlador. El kernel también actúa como una capa de abstracción entre el hardware y el resto de la pila de software(Shaheen, Asghar & Huss, 2017).

Las capas superiores se apoyan en el kernel de Linux para las funcionalidades subyacentes, como el subprocesamiento y la gestión de memoria de bajo nivel. Así Android aprovecha las características clave de seguridad y permite a los fabricantes desarrollar controladores de hardware para un Kernel bien conocido. (Training, 2017)

IPC corresponde a Inter-Process Comunication, se trata de una parte esencial para Android pues es la que permite a los procesos, las aplicaciones en ejecución, relacionarse con otros procesos de otras partes del sistema.

Android es un set de programas que trabajan en conjunto para producir un resultado. Los dispositivos Android utilizan el kernel de Linux que está modificado por Google en la arquitectura del kernel. La función principal del kernel es ser intermediario entre el software y el hardware.

[17] Bluetooth: Es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN)

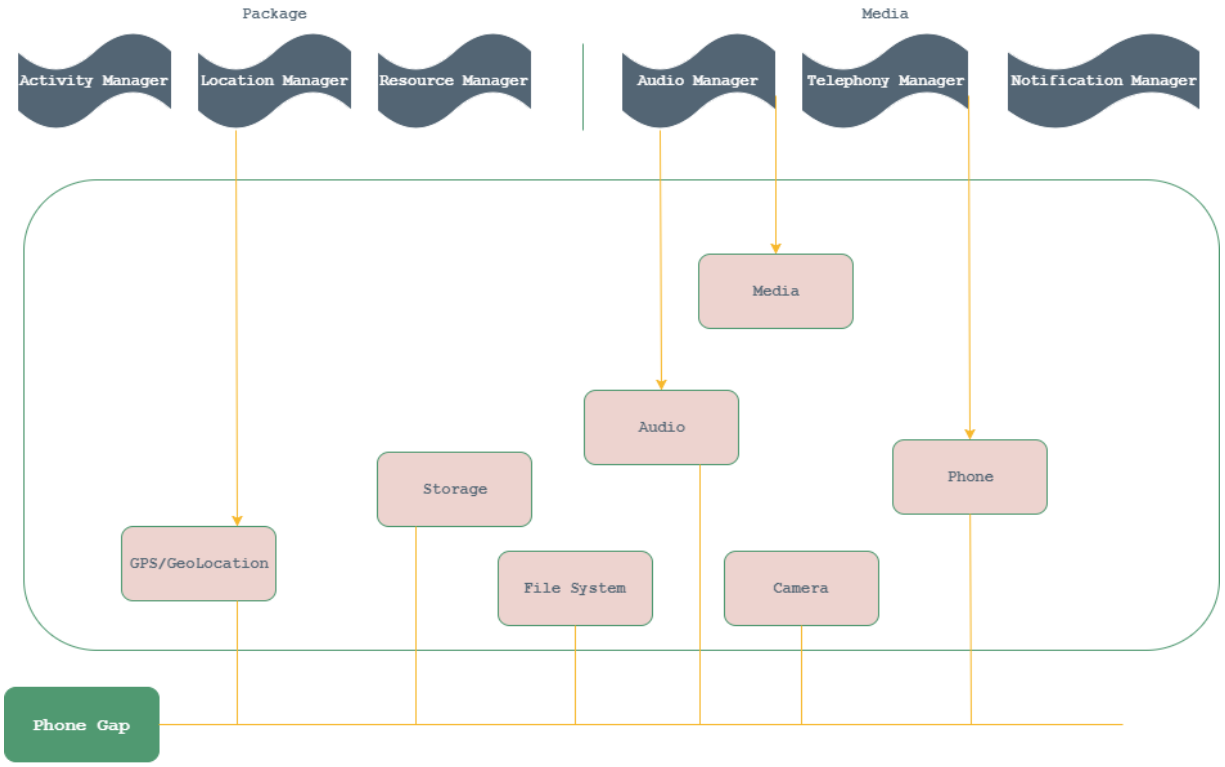

Ilustración 4: Paquetes incluidos en Android SDK para controlar hardware (Shan Khan, Naved Qureshi & Abdul Qadeer, 2014)

En el trabajo científico titulado "Mobile Theft Detection with Automatic Location Tracking By Android Application" se presenta una técnica para mejorar la detección de los robos en dispositivos Android mediante servicios como GPRS[18], Email, SMS[19], etc. En la ilustración 5 se presenta los paquetes utilizados del SDK para controlar el hardware. Como ejemplo p[a.7]aquete Location Manager utiliza la API GPS/GeoLocation para obtener la ubicación del dispositivo.

Android dispone de muchas APIs para proveer comunicación entre el hardware y el Kernel. Android Software Development Kit (SDK) dispone de herramientas y una larga lista de APIs para[a.8] desarrollar aplicaciones en la plataforma Android utilizando Java. El [a.9]Android SDK Manager contiene el código del Kernel de Android, librerías [a.10]nativas programadas en C/C++ y otros paquetes para comunicarse con el hardware. Esto permite el uso de

[18] Servicio general de paquetes vía radio: Es un punto de acceso que puede utilizar servicios de comunicación

[19] SMS: Es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos, conocidos como mensajes de texto

funcionalidades y características del dispositivo como cámaras, giroscopio, envió de mensajes, geolocalización, etc. (Shan Khan, Naved Qureshi & Abdul Qadeer, 2014).

1.4. Vulnerabilidades

La seguridad de las aplicaciones móviles y de las plataformas subyacentes en las que funcionan, se ha convertido en una gran preocupación para los investigadores y profesionales. Debido al impacto que los problemas de seguridad afectan a las plataformas móviles, esto causa problemas en la vida privada de las personas (por ejemplo, visualizar archivos privados), así como en las empresas (por ejemplo, interceptar decisiones comerciales estratégicas(Linares-Vasquez, Bavota& Escobar-Velasquez, 2017).

Para identificar vulnerabilidades y fortalecer los sistemas de software se requiere atención y esfuerzos constantes; sin embargo, eso es costoso y complicado analizar una base de códigos completa. Por lo tanto, es necesario priorizar los esfuerzos hacia las áreas vulnerables más probables.

En el trabajo científico titulado “Profiling Android Vulnerabilities” realiza un análisis manual de las vulnerabilidades de Android, utilizando la National Vulnerability Database (Base de datos nacional de vulnerabilidades), con el período 2008–2014 y enriqueciendo esta información con el sistema que proporciona una referencia para todas las vulnerabilidades informadas públicamente llamado Common Vulnerabilities and Exposures(CVE)(Jimenez, Papadakis, Bissyande & Klein, 2016).

Según el estudio las vulnerabilidades se presentan en la fase de código siendo la incorrecta implementación de un proceso y entradas no verificadas la mayor causa de las vulnerabilidades en aplicaciones Android, se puede apreciar con más detalle con la siguiente tabla:

Origin	Kind	Number	Total (%)
	Flow	4	
DESIGN	Insecure protocol	1	12 (27.90%)
	Unauthorized access	7	
	Resource Management		
	Buffer overflow	4	
	Incorrect pointer dereference	1	
	Stack consumption	1	
	Data		
	Input not verified	7	
CODE	Serialization issue	1	30 (69.77%)
	Semantic		
	Unprotected use of a function	3	
	Missing/incorrect implem. of a feature	11	
	Initialization		
	Object not rightly created	1	
	Wrong initialization of data	1	
TEST	Forgot to remove debug feature	1	1 (2.32%)

Ilustración 1: Distribución vulnerabilidades (Jimenez, Papadakis, Bissyande & Klein, 2016).

Umasankar en su trabajo científico titulado "Analysis of Latest Vulnerabilities in Android" analiza una base compuesta por datos de National Vulnerability Database, Open Web Application Security Project mobile top 10 (OWASP), Android Security Bulletings, y el sitio web de CVEDetails.

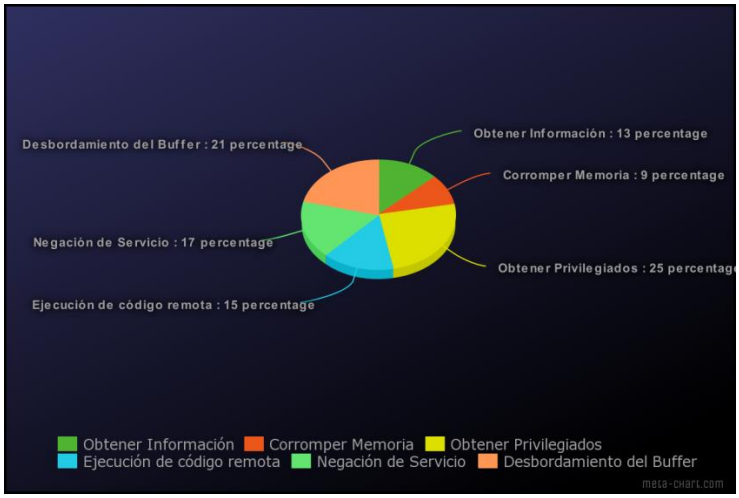

Ilustración 2: Gráfico de análisis de vulnerabilidad (Umasankar, 2017).

Concluye que el tipo de vulnerabilidad de salto de privilegio tiene la mayoría del 25%, la ejecución del código remoto es del 21%, la denegación de servicio del 17%, el desbordamiento de memoria del 15% (Umasankar, 2017).

Según el trabajo científico titulado "An Empirical Study on Android-related Vulnerabilities" las vulnerabilidades más frecuentes que afectan al sistema operativo Android son las relacionadas

a las que afectan la memoria con un 20% de una muestra de 510 vulnerabilidades (103 instancias), recopiladas de los Boletines de Seguridad oficiales de Android y del sitio web de CVE. Otras vulnerabilidades de importancia se relacionan con el manejo de datos típicamente encontrados en funcionalidades que procesan datos (74 instancias) y vulnerabilidades relacionadas con permisos, privilegios y controles de acceso (58 instancias).Finalmente, otras vulnerabilidades menos difundidas son aquellas que caen en las categorías: Validación de entradas incorrectas (51 instancias), características de seguridad (44 instancias), errores en los apuntadores (42 instancias), inicialización y errores de limpieza (33 instancias), control o manejo incorrecto de condiciones excepcionales (30 instancias), indicador de código de mala calidad (27 instancias), problemas de comportamiento (21), tiempo y estado (14), fallas de inyección (6), cumplimiento incorrecto del contrato API (4) y debilidades que afectan archivos o directorios 3 instancias). Se detalla en la ilustración 6.

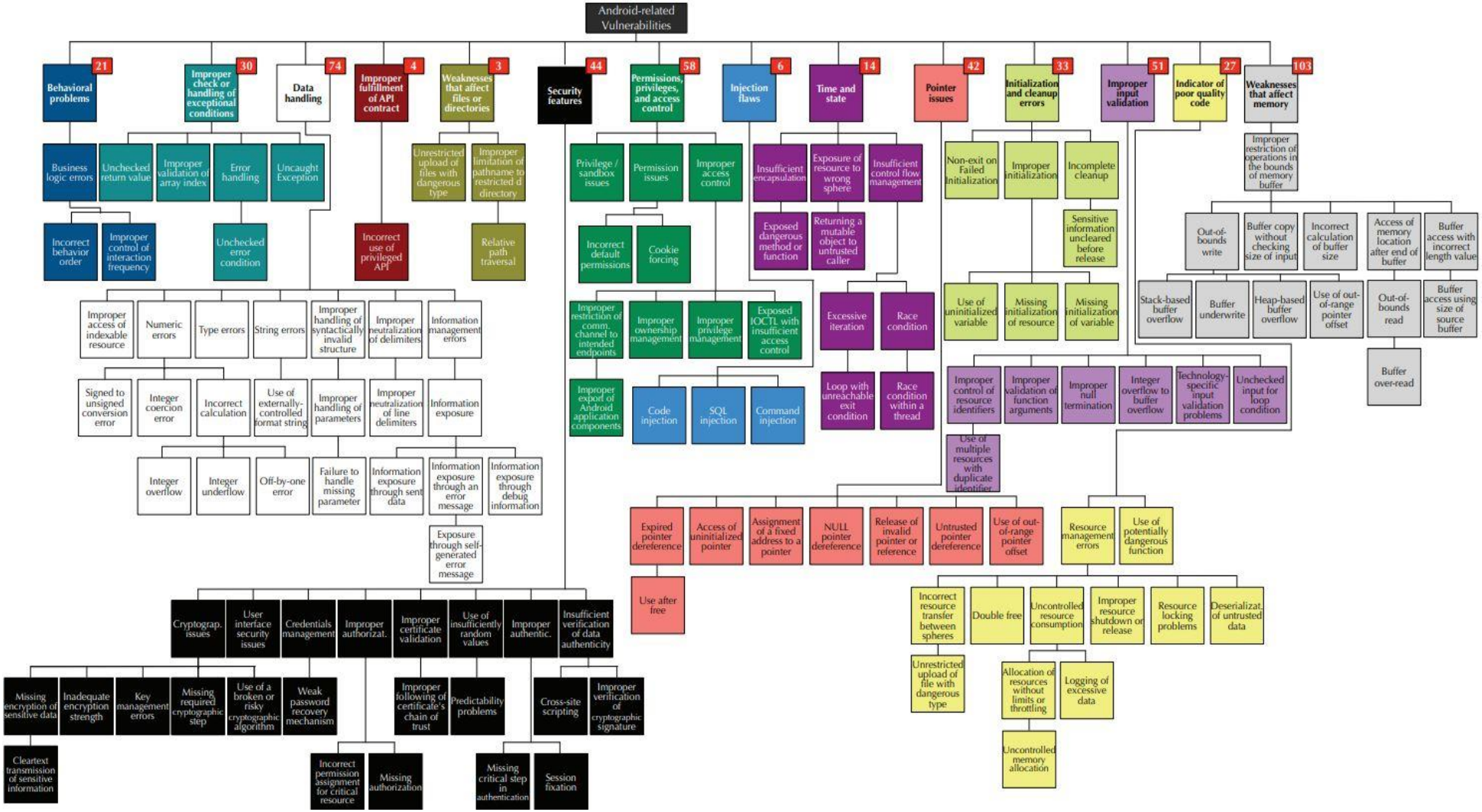

Ilustración 3: Tipos de vulnerabilidades relacionadas con Android (Linares-Vasquez, Bavota& Escobar-Velasquez, 2017).

El estudio también indica en que capa de la arquitectura Android se encuentran los errores. Se puede apreciar que los errores más comunes ocurren en la capa del Kernel de Linux. La mayoría de las vulnerabilidades afectan drivers de terceros. Los componentes de hardware más vulnerables son Drivers de video, Wifi y cámara.

La capa de librerías nativas es la segunda en exhibir múltiples vulnerabilidades. Esto se debe principalmente al subsistema Media Framework que ha sufrido 143 vulnerabilidades. El detalle en la siguiente ilustración:

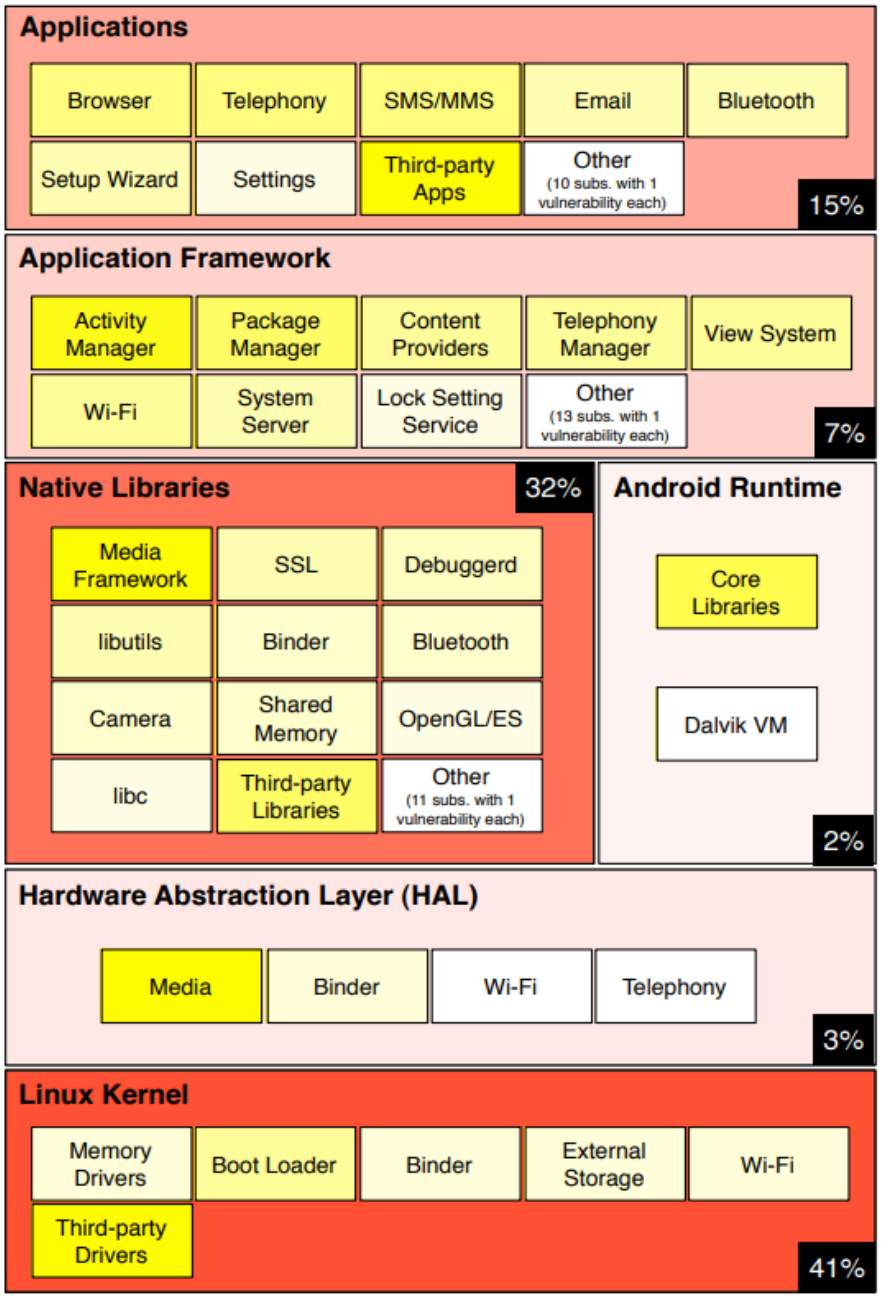

Ilustración 4: Mapa de calor de vulnerabilidades en las capas / subsistemas de Android (Linares-Vasquez, Bavota& Escobar-Velasquez, 2017).

La mayoría de las vulnerabilidades se pueden evitar recurriendo a prácticas de programación segura, especialmente en el contexto del manejo de datos y la asignación / acceso a la memoria. También, los desarrolladores podrían considerar el uso de lenguajes de programación modernos que incorporan mecanismos que promueven la programación segura y limpia.

2 Capítulo II: Identificación de protocolos y características que utilizan aplicaciones anti-robo[a.11]

La comercialización de teléfonos inteligentes ha introducido amenazas con respecto a la seguridad y la privacidad de los usuarios. Los dispositivos almacenan y procesan datos heterogéneos, que deben protegerse del acceso no autorizado. Los propietarios de estos dispositivos no son expertos en seguridad y, por lo tanto, pueden desconocer las amenazas y contramedidas pertinentes. En este trabajo se analizarán distintos protocolos, tecnologías y herramientas para realizar una comparación clara y precisa de cuáles son las mejores aplicaciones anti-robo gratuitas y pagadas para Android.

2.1. Aplicaciones Anti-robo

Con el transcurso del tiempo, las tecnologías de los dispositivos móviles se han desarrollado con una gran dinámica, tanto que han permitido facilitar la comunicación en diferentes áreas. Asimismo, se han simplificados procesos de trámites en línea. Sin embargo, aunque facilitan la calidad de vida del usuario, esta tecnología también se ha transformado en un blanco predilecto de atacantes informáticos y peor aún, robos físicos. Esto se explica no solo porque son equipos que pueden tener un elevado coste económico, sino también porque son utilizados para manejar servicios y productos bancarios o que involucran el uso de dinero ("Curso de seguridad en dispositivos móviles", 2017).

La mitigación principal contra el acceso no autorizado de datos en dispositivos robados es provista por aplicaciones anti-robo, mediante funciones de borrado y bloqueo remoto (University of Cambridge, 2015). De igual manera, estas aplicaciones están dotadas de funciones para rastreo, monitoreo, control remoto, sistema de alertas, guardar copias de seguridad en la nube, etc. Existen varias aplicaciones inteligentes anti-robo en el mercado; sin embargo, el único proyecto de código abierto, lo suficientemente grande, para competir con empresas como Cerberus Anti Theft es Prey es Open Source Theft Recovery.

Un trabajo interesante que está relacionado con el rastreo de dispositivos es “Security Analysis of Consumer-Grade Anti-Theft Solutions Provided by Android Mobile Anti-Virus Apps”, en él se estudian los mecanismos anti-robo disponibles que tienen los consumidores para frustrar el

acceso no autorizado a los datos personales de teléfonos inteligentes Android que son robados.

Entre los mecanismos más importantes se incluye bloquear el dispositivo remotamente, eliminar la información del dispositivo remotamente, geolocalización remota mediante APIs (La más común Google Maps), envío de mensajes SMS y MMS, autenticación de usuarios, logs[20], deshabilitar sincronización de datos y bloquear dispositivo por número de intentos.

El presente algoritmo representa un funcionamiento general de las aplicaciones anti-robo, cabe recalcar que este algoritmo vario dependiendo las funcionalidades y prioridades de la aplicación.

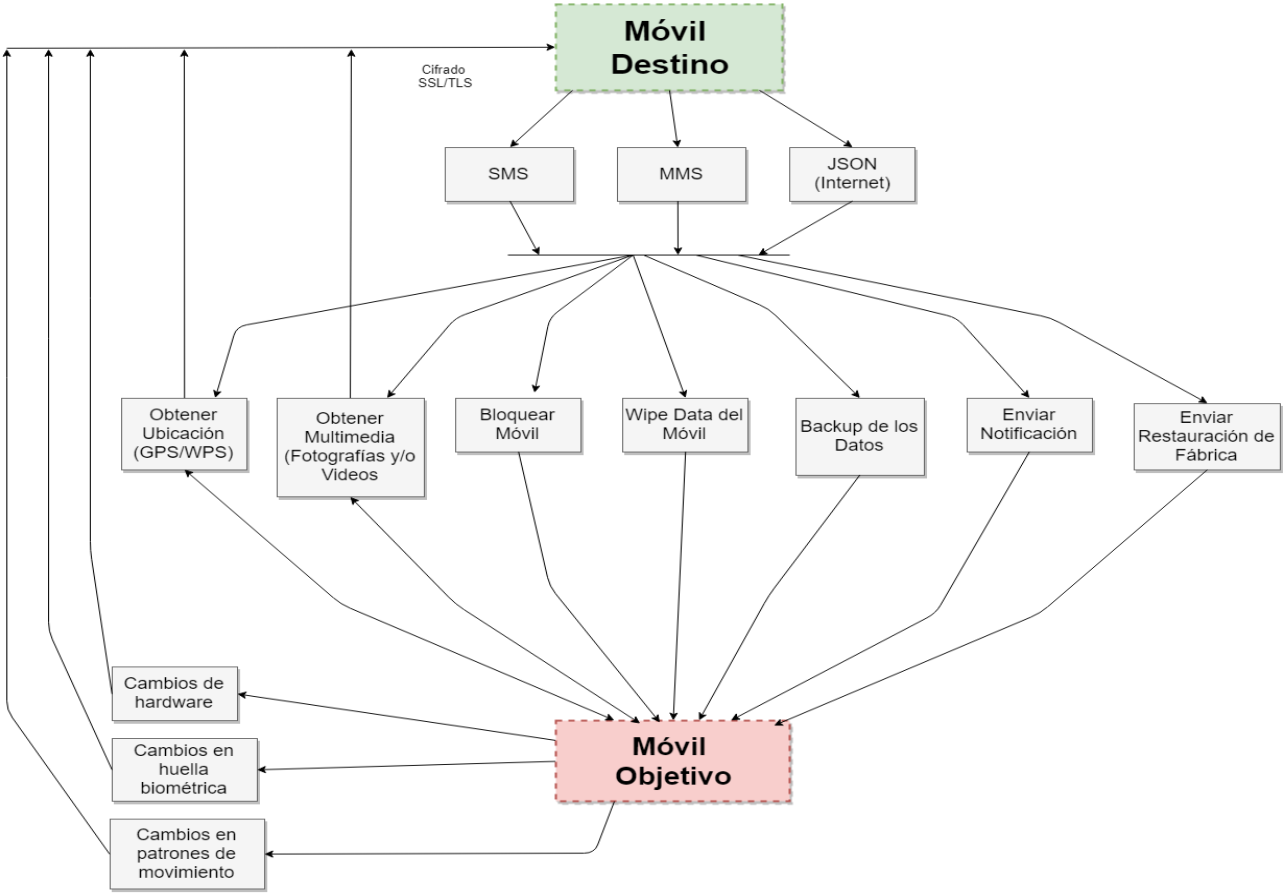

Ilustración 5: Representación algoritmo aplicaciones anti-robo

2.1.1. Secure Socket Layer (SSL) y Transport Layer Security(TLS) [a.12]

[20] Logs: Registro de la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular

Los desarrolladores de aplicaciones móviles están enfrentando un nuevo y difícil reto de seguridad. Mientras las aplicaciones web tradicionales, comunes de escritorio, dependen del navegador web para administrar la seguridad de las comunicaciones, cada aplicación móvil debe cuidar de este elemento por su propia cuenta. Estableciendo un canal seguro utilizando el protocolo SSL/TSL, requiere que el cliente valide la certificación SSL que se envía a través del servidor (Gagnon, 2015).

SSL[21]y TLS[a.13][22]han sido un estándar como medio para transferir datos de forma segura a través de redes no confiables como Internet. Son comúnmente usadas para el cómputo general, donde una o más partes, o direcciones IP[23], se conocen antes de la conexión y las conexiones son generalmente transitorias.

Mientras que Transpor tLayer Security (TLS) es el sucesor del protocolo Secure Sockets Layer (SSL) y el estándar de la industria dominante; ambos son protocolos criptográficos que proporcionan comunicaciones seguras en Internet para cosas tales como navegación web, acceso a la nube, comunicaciones por correo electrónico, mensajería instantánea y otras transferencias de datos. Existen ligeras diferencias de funcionalidad entre SSL y TLS, y SSL es, a sabiendas, menos seguro que TLS actualmente, pero los protocolos siguen siendo sustancialmente los mismos (A Technology Brief on SSL/TLS Traffic, 2016).

El flujo básico de un SSL Handshake (comunicación cliente/servidor) es que primero el cliente enviará[a.14] un mensaje “Hola Cliente”, al cual el servidor responde con otro mensaje “Hola Servidor”. En este punto la validación del certificado y los parámetros criptográficos ocurren. (Trummer & Dalvi, 2015)

Pasos que permiten que el cliente (aplicación anti- robo) y el servidor SSL o TSL se comuniquen entre sí:

1. Quedar de acuerdo en que versión del protocolo utilizar
2. Seleccionar algoritmos criptográficos
3. Autenticación mutua intercambiando y validando certificados digitales
4. Uso de técnicas de encriptación asimétrica para generar una clave secreta compartida
5. SSL o TLS luego utiliza la clave compartida para el cifrado simétrico de mensajes que es mucho más rápido que el cifrado asimétrico ("IBM Knowledge Center", 2017)

[21] SSL (Secure Sockets Layer): Es la tecnología de seguridad estándar para establecer un enlace encriptado entre un servidor web y un navegador.

[22] TLS (TransportLayer Security): Proporciona privacidad e integridad de datos entre dos aplicaciones que se comunican. A diferencia de SSl, este protocolo admite algoritmos más nuevos y más seguros.

[23] IP: Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo

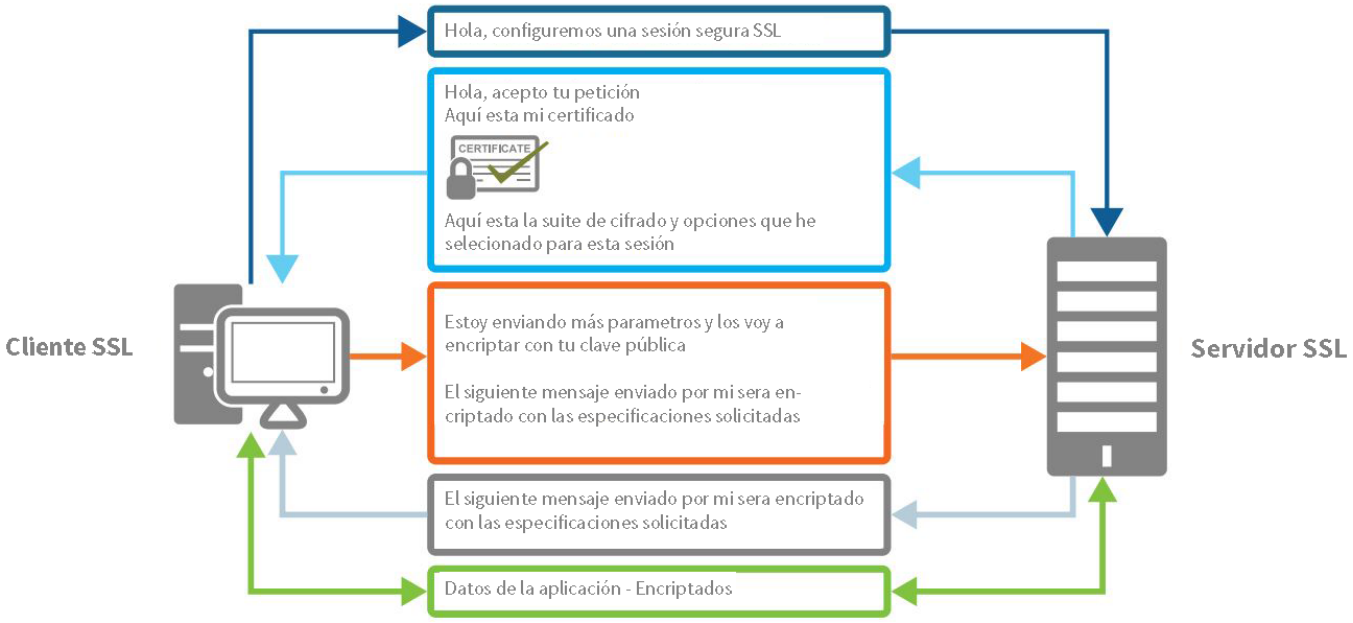

Ilustración 6: Ilustra la secuencia de transacciones SSL (Raymond &Sushmitha, 2017)

La seguridad en los servidores de aplicaciones anti-robo es crítica. Si el servidor es hackeado por ciberdelincuentes, la base de datos de todos los usuarios que utilizan aplicaciones anti-robo está comprometida. Algunos canales de comunicación entre el servidor y el cliente de aplicaciones anti-robo no están encriptadas con estándares SSL/TLS. Esto implica que se pueden realizar ataques Man in the Middlec (MitM)[24], visualizar contraseñas (sniffing)[25], secuestros de sesión, escuchar todas las comunicaciones (Eaves dropping)[26] y modificar los datos de los usuarios (Raymond & Sushmitha, 2017).

Para que las aplicaciones anti-robo puedan utilizar los protocolos SSL/TLS el servidor se configura con un certificado que contiene una clave privada y una pública coincidente. Como parte del acuerdo entre un servidor y un cliente SSL, el servidor confirma que tiene la clave

[24] Ataque de intermediario: Es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad

[25]Sniffer: Es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador

[26] Ataque de canal lateral: Es un ataque basado en información obtenida gracias a la propia implementación física de un sistema informático

privada firmando su certificado con criptografía de clave pública (Seguridad con HTTPS [27]y SSL, 2018).

Según las políticas de seguridad la mayoría de las aplicaciones anti-robo son bastantes seguras en la actualidad, y se basan principalmente en la seguridad estándar SSL y TLS(Lee, 2016).

2.1.2.SMS (Short Message Service)

Las aplicaciones anti-robo deben ejecutar instrucciones y enviar información al propietario en caso de robo. Los mensajes SMS permiten realizar esto sin estar conectado a Internet. Es considerado una segunda medida para realizar operaciones a distancia en el dispositivo inteligente.

Markovski muestra cómo funcionan los mensajes SMS en su investigación científica titulada "A Protocol for Secure SMS Communication for Android OS", los mensajes SMS se envían a través de un mecanismo de almacenamiento y reenvío a un Centro de servicio de mensajes cortos (SMSC), que intentará enviar el mensaje al destinatario y posiblemente volverá a intentarlo si el usuario no es accesible en un momento dado. La transmisión de los mensajes cortos entre SMS y teléfono se realiza a través del sistema de señalización número 7 (SS7) dentro del protocolo no encriptado que permite a los empleados de la red de proveedores de telefonía móvil, que tienen acceso a la red SS7, interceptar o modificar mensajes SMS (Markovski, Kuzmanovska & Simeonovski, 2012).

2.1.3.MMS (Multimedia MessagingService)

El usuario requiere de mucha información para poder rastrear el dispositivo móvil, no obstante, él envió de mensajes SMS es muy limitado ya que solo acepta texto. Esta tecnología permite enviar contenido multimedia como videos y fotografías, fundamental para rastrear al delincuente del dispositivo inteligente (ARCHANA, BHUVANESHWARI & HEMAVATHI, 2015).

Las aplicaciones anti-robo utilizan MMS para monitorear constantemente al delincuente del dispositivo inteligente. La ventaja de tener la tecnología MMS trabajando en conjunto con el servicio de mensajería SMS, brinda al usuario toda la información que requiere en poco tiempo

[27] Protocolo seguro de transferencia de hipertexto: Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto

En el trabajo de investigación titulado “Multimedia Messaging Service(MMS) Based Anti theft Application”, se accede a los servicios MMS e Internet desde el móvil para enviar los archivos multimedia al número de teléfono alternativo y también al correo. El número de SIM actual y la ubicación también se envía al número alternativo como un SMS (Archana, Bhuvaneshwari & Hemavathi, 2015).

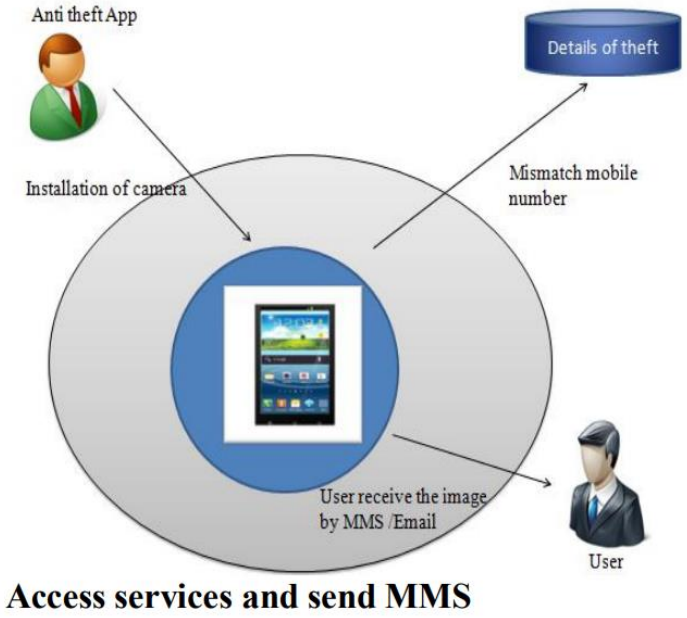

Ilustración 7: Acceder a servicios y enviar MMS (Archana, Bhuvaneshwari & Hemavathi, 2015)

2.2. Huellas biométricas

La ventaja de la autenticación biométrica mediante huellas dactilares sobre otra autenticación biométrica es la singularidad y el alto rendimiento. Todas las personas en el mundo tienen una única huella digital, dos personas no pueden tener la misma huella digital, ni siquiera los gemelos (Kuriakose& K, 2017).

Las aplicaciones anti-robo guardan las huellas biométricas de los usuarios malintencionados, la policía puede utilizar esta información para identificar y capturar al ladrón. Para desarrollar un sistema autónomo, se puede integrar una nueva biblioteca en el ecosistema de Android. SourceAFIS es una biblioteca que se utiliza para reconocimiento / coincidencia de huellas dactilares. La funcionalidad esencial del Sistema de Identificación Automática (AFIS) consiste en comparar dos huellas dactilares y decidir si pertenecen a la misma persona. SourceAFis proporciona una búsqueda rápida en una base de datos de huellas digitales registradas. Viene

con una API fácil de usar (.NET puro y un puerto experimental de Java) y aplicaciones y herramientas complementarias (Dospinescu & Lîsîi, 2016).

Con un lector de huellas dactilares se pueden obtener imágenes en alta calidad para ejecutar algoritmos mediante la biblioteca SourceAFIS, esta biblioteca procesa la imagen de la huella mediante un algoritmo para poder realizar la comparación (Dospinescu & Lîsîi, et al).

La investigación científica titulada "Secured Android Application Using Biometric Authentication" propone un sistema de autenticación biométrica de tres fases. La primera fase trata de guardar la huella biométrica por primera vez y actualiza los factores. La segunda fase es el mecanismo de como guarda la huella en el almacén de claves. La tercera fase es el mecanismo de ingreso (Kuriakose & K, 2017).

2.3. Sensores de Movimiento

La mayoría de los dispositivos con Android tienen sensores incorporados que miden el movimiento, la orientación y varias condiciones ambientales. Estos sensores son capaces de proporcionar datos en bruto con alta precisión y precisión, y son útiles si desea monitorear el movimiento o posicionamiento tridimensional del dispositivo, o si desea monitorear cambios en el entorno ambiental cerca de un dispositivo (Overview, 2018).

Las aplicaciones que utilizan sensores de movimiento adoptan una metodología de aprendizaje de máquina, consiste en una fase de entrenamiento. Primero se recolecta información de cómo el usuario realiza los movimientos con el dispositivo inteligente, específicamente de cómo lo levanta del bolsillo o bolso. Los lectores del acelerómetro y sensor del giroscopio distinguen los movimientos del propietario y el algoritmo los clasifica de los movimientos anormales de usuarios malintencionados. Estos clasificadores se entren con clasificadores más fuertes utilizando el algoritmo AdaBoost para aumentar la precisión. Esta funcionalidad utiliza el clasificador fuerte preentrenado para verificar la legitimidad de los intentos de captación de un usuario, y desbloquea el dispositivo inteligente si el usuario pasa la verificación. De lo contrario, el algoritmo tratará los intentos como eventos inusuales, lo que implica que se está produciendo un robo. En consecuencia, se activa una alarma de inmediato. La idea detrás de los sensores de movimiento es que las personas tienen características fisiológicas consistentes y distintivas (por ejemplo, la estructura física del brazo) y características de comportamiento (por ejemplo, patrones de comportamiento de captación) (Chang, Lu & Song, 2016).

2.4. APIs de Geolocalización

La popularidad de los mapas digitales ha crecido rápidamente en los últimos años. Si bien Google sigue siendo el líder en lo que respecta a los mapas con Google Maps, ahora hay muchas otras compañías en la industria de la tecnología de mapas. Los mapas pueden ser útiles, informativos, creativos cuando se trata de integrar esta tecnología a las aplicaciones anti-robo.

2.4.1 Google Maps

Las aplicaciones anti-robo utilizan la API de Google MapsGeolocation por su radio de precisión y facilidad en la implementación con aplicaciones Android. Esta API devuelve la ubicación en función de información acerca de torres celulares y nodos de WiFi que el cliente móvil puede detectar. La comunicación se realiza a través de HTTPS usando el método POST. Tanto la solicitud como la respuesta poseen formato JSON (Google MapsGeolocation API | Google MapsGeolocation API | Google Developers, 2018).

Las aplicaciones anti-robo pueden agregar mapas basados en datos de Google Map. La API administra en forma automática el acceso a servidores, descargas de datos, visualización de mapas y respuesta a gestos de mapas de Google Maps (Introducción a la Google Maps Android API | Google Maps Android API | Google Developers, et. al).

2.4.2 Microsoft Bing Maps

La plataforma Bing Maps proporciona múltiples opciones de API para su aplicación, incluido Control Web, un control de aplicaciones de la Tienda Windows, un control WPF, Servicios REST y Servicios de Datos Espaciales.

Para dispositivos Android la interfaz de programación de aplicaciones (API) REST Services de Bing Maps proporciona una interfaz Representational State Transfer (REST) para realizar tareas tales como crear un mapa estático con marcadores, geocodificar una dirección, recuperar metadatos de imágenes o crear una ruta (Bing Maps REST Services, 2018).

2.4.3 OpenLayers

OpenLayers es una biblioteca de JavaScript [28]de código abierto que utiliza WebGL, Canvas 2D y otras características HTML5 para renderizar mapas en navegadores web modernos. OpenLayers es capaz de extraer mosaicos de OpenStreetMap, Bing, MapQuest, Stamen y muchas otras fuentes de mapeo. OpenLayers también es capaz de representar datos vectoriales de GeoJSON, TopoJSON, KML, GML y otros formatos de datos geográficos. (OpenLayers - Welcome, 2018)

Sin embargo, la API más utilizada para dispositivos Android es Google Maps ya que proporciona documentación de API muy detallada, así como muestras de código, bibliotecas, SDK y otras herramientas de mapeo digital. También hay un selector de API que los desarrolladores pueden usar para encontrar la API de mapeo adecuada para sus proyectos.

2.4.4 Sistema de posicionamiento WiFi (WPS)

Los WPS se utilizan cuando el posicionamiento GPS no funciona adecuadamente debido a los bloqueos de señal en interiores o bajo tierra. El WPS aprovecha que las redes de WiFi están creciendo rápidamente en número y, por lo tanto, se pueden utilizar tanto para el acceso hacia la red como para la geolocalización, reduciendo la necesidad de inversiones en infraestructura.

Los dispositivos con WiFi y GPS se pueden usar para enviar información sobre una red WiFi a un proveedor de servicios de ubicación (Google). Esto permite determinar dónde se encuentra la red WiFi en particular. Esto se hace haciendo que el dispositivo envíe la dirección MAC[29]del punto de acceso junto con la ubicación determinada por el GPS. Si el GPS se usa para determinar la ubicación de un dispositivo, también escaneará las redes cercanas que pueden usarse para identificar la red. Cuando encuentre la ubicación de las redes WiFi, la información se registrará para el acceso público. La próxima vez que alguien esté cerca de una de esas redes WiFi, pero carezca de una señal de GPS, este servicio se usará para determinar una ubicación a medida que se registra la ubicación de la red (About Wi-Fi Positioning - Combain, 2018).

La forma en que esto funciona es haciendo que el dispositivo envíe el BSSID del punto de acceso (dirección MAC) junto con la ubicación determinada por el GPS.

[28]Javascript: Es un lenguaje de programación interpretado orientado a objetos

[29] Media Access Control: Es un identificador de 48 bits (6 bloques de dos caracteres hexadecimales (4 bits) que corresponde de forma única a una tarjeta o dispositivo de red

Cuando se utiliza el GPS para determinar la ubicación de un dispositivo, también escanea las redes cercanas para obtener información de acceso público que se puede utilizar para identificar la red. Una vez que se encuentran la ubicación y las redes cercanas, la información se registra en línea. De esta manera si el dispositivo no tiene señal GPS puede utilizar la información de la base del proveedor del servicio para posicionar la ubicación (Zahradnik, 2017).

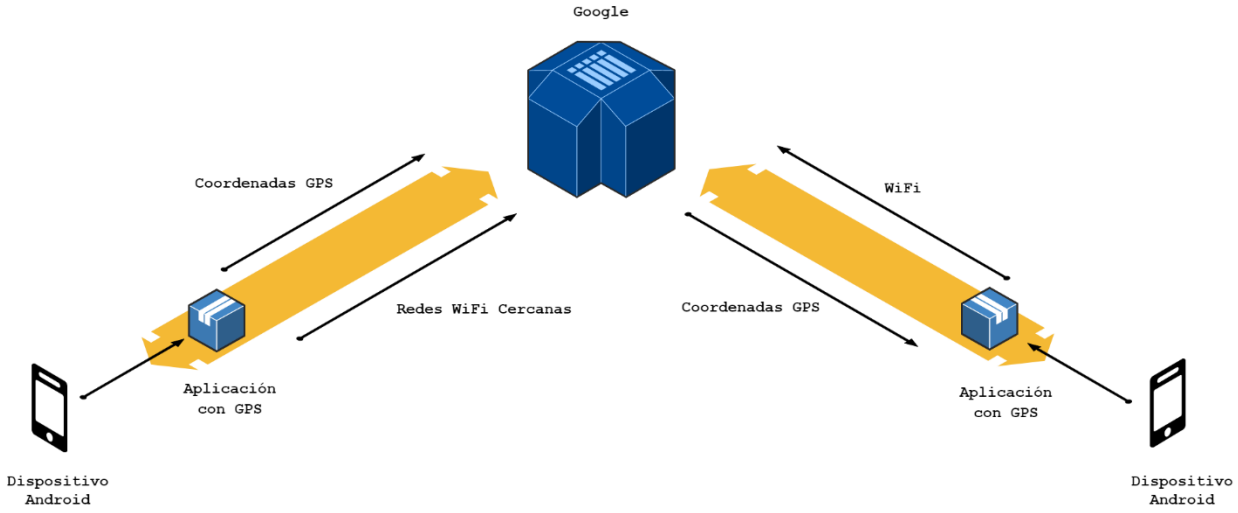

Ilustración 8: Sistema de Posicionamiento WiFI (WPS)

2.5. Capturar fotografías y videos silenciosamente

Las aplicaciones anti-robo requieren de funcionalidades que actúen de la manera más discreta posible, esto implica que las aplicaciones deben ser lo más silenciosas y no deben advertir al usuario malintencionado que los están espiando.

Android proporciona varias herramientas y librerías para controlar la cámara, capturas de pantalla y grabadora del dispositivo.

El SDK de Android proporciona librerías para manipular la cámara del dispositivo. Antes de realizar tomas fotográficas, toda aplicación verifica que la cámara se encuentre disponible y el número de cámaras disponibles en el dispositivo (frontal o trasera)[a.15]. Para realizar este proceso se debe declarar permisos necesarios en el archivo de manifiesto para que el usuario pueda autorizar el uso de cámara en la aplicación(Shedge, Dhatrak&Ugale, 2017).

Con la ayuda del *Framework* de Android se puede utilizar distintas APIs para realizar capturas fotográficas. Camera Intent es una manera rápida de utilizar la aplicación de la cámara, proporciona una acción para solicitar la imagen o video de nuestra cámara. Luego está es guardada en la tarjeta SD. Para obtener la ubicación del archivo se lo guarda en el almacenamiento externo (Shan Khan, Qureshi & Qadeer, 2014).[a.16]

Para grabar el sonido del video se requiere de la API Media Recorder. El *Framework* multimedia de Android incluye soporte para capturar y codificar una variedad de formatos comunes de audio y video. Puede usar las API de MediaRecorder si el hardware del dispositivo lo admite (MediaRecorder | Android Developers, 2018).

La Api contiene una clase de Android llamada Media Recorder que permite grabar audios y videos. El control de grabación se basa en una máquina de estado simple(MediaRecorder | Android Developers, n.d.)

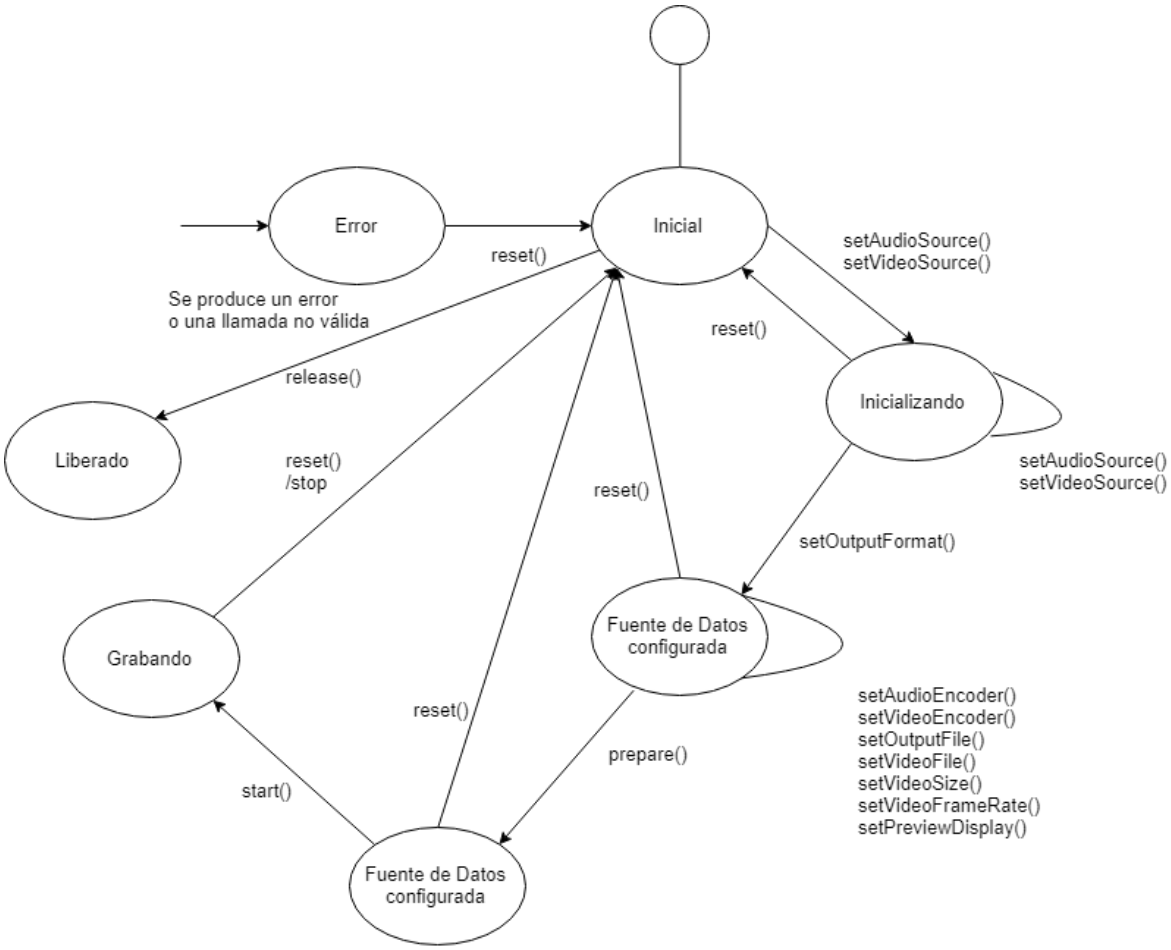

Ilustración 9: Diagrama de estado de la clase MediaRecorder (Shan Khan, Qureshi & Qadeer, 2014)

2.6. RemoteWipe Data

Según el gobierno del Reino Unido se informa que casi 5100 teléfonos móviles se perdieron y causaron pérdidas financieras por valor de 2.000 millones de dólares a esa compañía por los datos confidenciales de la empresa. Según un estudio reciente de Vanson Bourne, se confirma que casi el 40% de los empleados de las empresas perdieron sus teléfonos móviles que contienen información crítica para el negocio (Chowdhury&Ghosal, 2015).

Una solución es eliminar automáticamente los datos confidenciales después de una serie de intentos fallidos de autenticación. Sin embargo, puede causar la eliminación accidental de datos cuando el propietario olvida la contraseña o alguien juega con el teléfono de otra persona. Además, un adversario aún puede acceder a los datos confidenciales conectando el teléfono inteligente a una PC (Yu, 2014).

Las soluciones existentes dependen de una conexión a internet o una red celular para enviar los comandos de borrado; sin embargo, existen mecanismos que permite en enviar comandos a través de la red de emergencias. Un estudio realizado en 2014 que está relacionado con el RemoteWipe Data[30](Borrado Remoto de los Datos) es "Remotely Wiping Sensitive Data on Stolen Smartphones", se propone un mecanismo que permite a los propietarios eliminar de manera remota un dispositivo inteligente incluso sin red WiFi y con la tarjeta SIM desconectada. La idea básica es permitir que el dispositivo inteligente use el canal de llamadas de emergencia de la red celular para recibir comandos remotos siempre y cuando existe cobertura GSM (Yu et al., 2014).

[30]Wipe Data: Es un algoritmo de eliminación de datos

3. Capítulo III: Comparación entre las diferentes aplicaciones anti-robo

Esta comparación proporciona las características fundamentales y reseñas de las aplicaciones anti-robo más importantes y eficientes en el mercado. Todas las aplicaciones corren en el sistema operativo Android de Google. Esta comparación tiene como objetivo ayudar a los lectores a decidir si se beneficiaran de las características de seguridad más sofisticadas proporcionadas por una aplicación.

La revisión se centra en las características de seguridad (anti-robo) y solo menciona funcionalidades adicionales brevemente. La estructura de cada informe de producto es idéntica, lo que permite a los lectores comparar productos fácilmente. Además, una breve tabla al final de cada informe del producto brinda una descripción general de las funciones.

Un componente anti-robo en una aplicación puede ser utilizado para recuperar el dispositivo, prevenir acceso a información privada almacenada en el dispositivo, obtener capturas multimedia del ladrón, enviar notificaciones, etc.

Al final de la introducción, se enlista las aplicaciones anti-robo participantes. A continuación, se incluyen revisiones detalladas de los productos individuales, en las cuales se arrojarán luz sobre el diseño y el uso de las características. En la tabla que representa las características anti-robo de un producto, se comenta brevemente cada función y se utiliza los siguientes símbolos para indicar qué tan bien funcionó a las pruebas.

Problema(s) Mayores

Problema(s) Menores

Funciona correctamente

Aplicaciones probadas:

- FindmyDevice
- Cerberus
- Prey
- Avast Anti-Theft
- Where'smyDroid

3.1. Encontrar mi dispositivo – Google (2017)

Si un dispositivo Android es extraviado o robado, se puede ubicar, bloquear, o borrar la memoria del teléfono inteligente. Encontrar mi dispositivo está funcionando predeterminadamente en los dispositivos Android asociados a una cuenta de Google. Incluye teléfono o Tablet Android, o un reloj Wear.

Funciona de manera similar a otras apps anti-robo como Preyo Cerberus. Encontrar mi dispositivo es una aplicación exclusivamente para dispositivos Android y es gratuita en Google Play Store.[a.17]

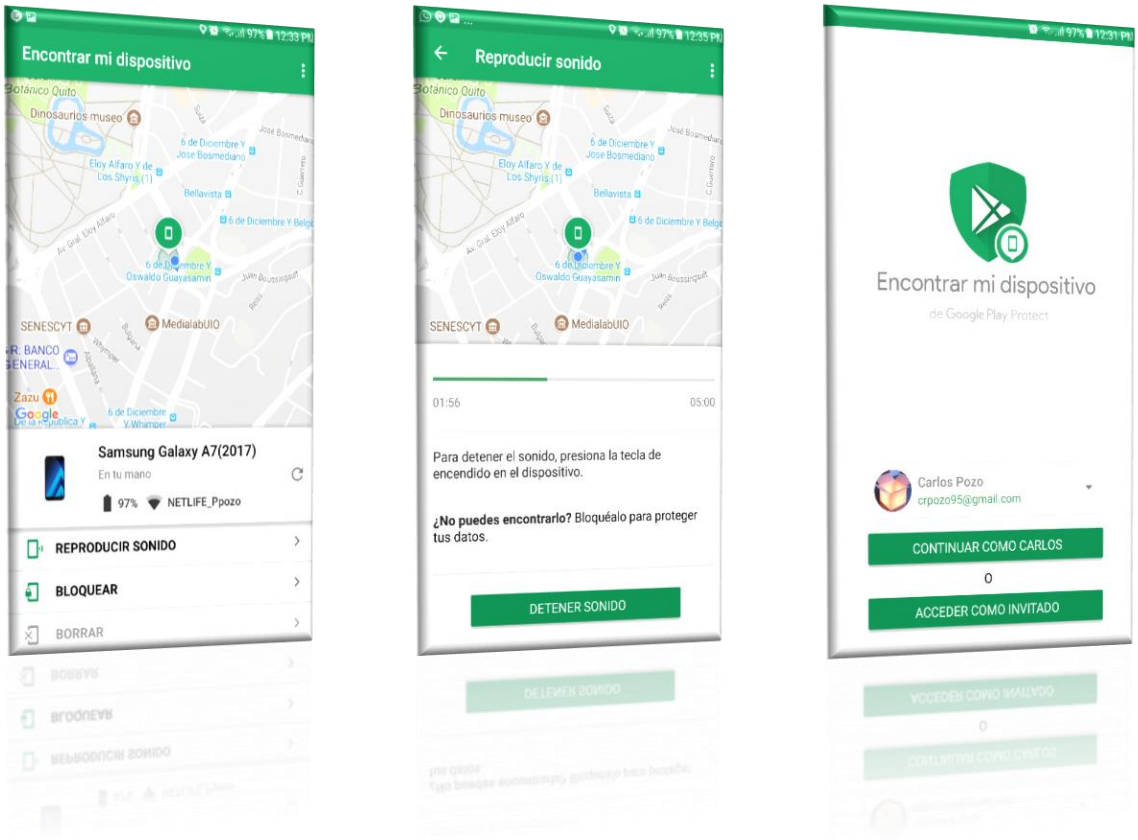

Ilustración 10: Pantallas Encontrar mi Dispositivo de Google

Manejo

Para usar Encontrar mi dispositivo, su dispositivo perdido debe ser:

- Encendido
- Ha iniciado sesión en una cuenta de Google
- Conectado a datos móviles o Wi-Fi
- Visible en Google Play

- Ubicación activada
- Encontrar mi dispositivo encendido

Después de instalar la aplicación en el dispositivo, el usuario es inmediatamente dirigido al inicio de sesión de la cuenta de Google con opción a registrar una cuenta de Google. Una vez se inicia sesión con la cuenta de Google se pregunta al usuario si puede acceder a la ubicación del dispositivo. Al habilitar el permiso se despliega un mapa con la ubicación del teléfono y tres funciones anti-robo. La primera es reproducir una alarma por 5 minutos en el dispositivo, la segunda es bloquear el dispositivo con opción a enviar un mensaje en la pantalla bloqueada y un número de teléfono opcional para poder contactarse, por último, la función de borrado que elimina toda la información del dispositivo.

Características importantes

- Encuentra tu teléfono, Tablet o reloj: El servicio de geolocalización de Google encontrara el dispositivo en segundos
- Reproduce un sonido: Con esta aplicación puedes proteger el dispositivo de forma remota y permitir que alguien que se ponga en contacto contigo
- Bloquea el dispositivo, borra sus datos o muestra un mensaje: Proteger el dispositivo de forma remota y permitir que alguien se ponga en contacto contigo
- Permite asegurar varios dispositivos Android
- La aplicación dispone de un administrador web para accionar diferentes funcionalidades como bloquear, localizar, hacer sonar una alarma, cerrar sesión de la cuenta Google, ponerse en contacto con el proveedor de telefonía, borrar el contenido y llamar al dispositivo

Detalles anti-robo[a.18]

Esta tabla proporciona indicadores clave para medir funcionalidades de la aplicación en términos anti-robo dividido entre funcionalidades principales y secundarias. Entre otras cosas esta tabla trata de ayudar a los lectores a decidir si se beneficiaran de las características de seguridad más integrales y sofisticadas.

Tabla 2: Detalles Anti-robo Encontrar mi Dispositivo

Detalles Anti-robo		
Características Principales		
Alarma		El ladron puede apagar el sonido con solo tocar el dispositivo
Borrado		Según el fabricante existe la posibilidad de que no sea posible eliminar el contenido de la tarjeta SD
Bloqueo		Permite enviar mensajes y llamar desde el dispositivo perdido al número de contacto establecido
Geolocalización		Sin internet no se puede localizar el dispositivo. Se visualiza el historial de las rutas en donde estuvo el dispositivo mediante Rutas de Maps
Capturas de pantalla		No permite el envío de capturas de pantalla
Fotografías		No toma fotografias de la cámara trasera o frontal del dispositivo
Grabar Videos		No permite grabar videos con la cámara trasera o frontral del dispositivo
Grabar Audio		No permite grabar audio con el microfóno del dispositivo
Características Adicionales		
Modo Incognito		See visualiza el icono de la app en la barra de notificaciones
Forwarding		Todas las llamadas y mensajes no se envían a un número establecido
Multiplataforma		La app funciona para dispositivos Android exclusivamente. Móviles, Tablets, Phablets y SmartWatches
Dashboard Web		Se puede visualizar la ubicación del dispositivo en un mapa y enviar acciones a la aplicación
Envío de acciones		Solo puede enviar acciones a la aplicación por Internet. No existe el envío mediante SMS y MMS
Activar/Desactiar Funciones		No permite desactivar y activar ninguna función
Terminal de Android		No permite enviar comandos especializados a traves del shell de Android
Obtener información del dispositivo		Despliega información muy limitada como la bateria y el nombre de la red Wi-Fi
Modo Emergencia		No soporta modo emergencia
Fake Shutdown		No soporta esta funcionalidad
Iniciar Aplicación / Servicios		No permite el inicio de aplicaciones y servicios remotamente
Copias de Seguridad		No permite descargar contactos y tampoco registro de llamadas

Ventajas

- Se vincula el dispositivo con una cuenta de Google manteniendo todo en una misma plataforma
- El rastreo del dispositivo es muy eficiente. La aplicación funciona con distintos servicios de Google como Rutas de Google Maps, permite obtener un historial de ubicación cada minuto del dispositivo
- El bloqueo envía un mensaje personalizado con un número de contacto para facilitar la recuperación del dispositivo
- La aplicación es multiplataforma exclusivamente en dispositivos Android. Se instalar en móviles, tablets, phablets y smartwatches

- La aplicación funciona en conjunto con un dashboard web que permite visualizar el dispositivo en un mapa y enviar acciones

Desventajas

- Tener una cuenta de Google
- Debe estar prendido el dispositivo
- Conectado a datos móviles o Wifi
- Activar la función ubicación en configuraciones
- Una vez que borres el contenido del dispositivo, no podrás utilizar Encontrar mi dispositivo
- La aplicación no permite realizar capturas de pantalla ni tomar fotografías desde la cámara frontal o trasera, grabar vídeos y grabar audios con él micrófono. Esto dificulta la investigación del ladrón
- No existe un modo incognito. El ladrón puede eliminar la aplicación rápidamente para evitar acciones en contra de su voluntad
- No existe un desvío de llamadas y mensajes. Todo lo que el ladrón envíe no puede ser controlado por el propietario
- El envío de acciones solo puede ser mediante Internet

3.2. Cerberus App

Cerberus es una aplicación anti-robo muy completa, proporciona protección a dispositivos Android para recuperar teléfonos inteligentes basados en Android extraviados o robados. Cerberus tiene muchas características únicas que lo convierten en la aplicación perfecta para localizar un teléfono o tablet, identificar al ladrón y recuperar su dispositivo.

Es una aplicación muy sofisticada y con una interfaz muy amigable. No obstante, el código fuente no es abierto (Cerberus anti theft–oficial website, 2017). Un código fuente cerrado limita el desarrollo e innovación de la aplicación.[a.19]

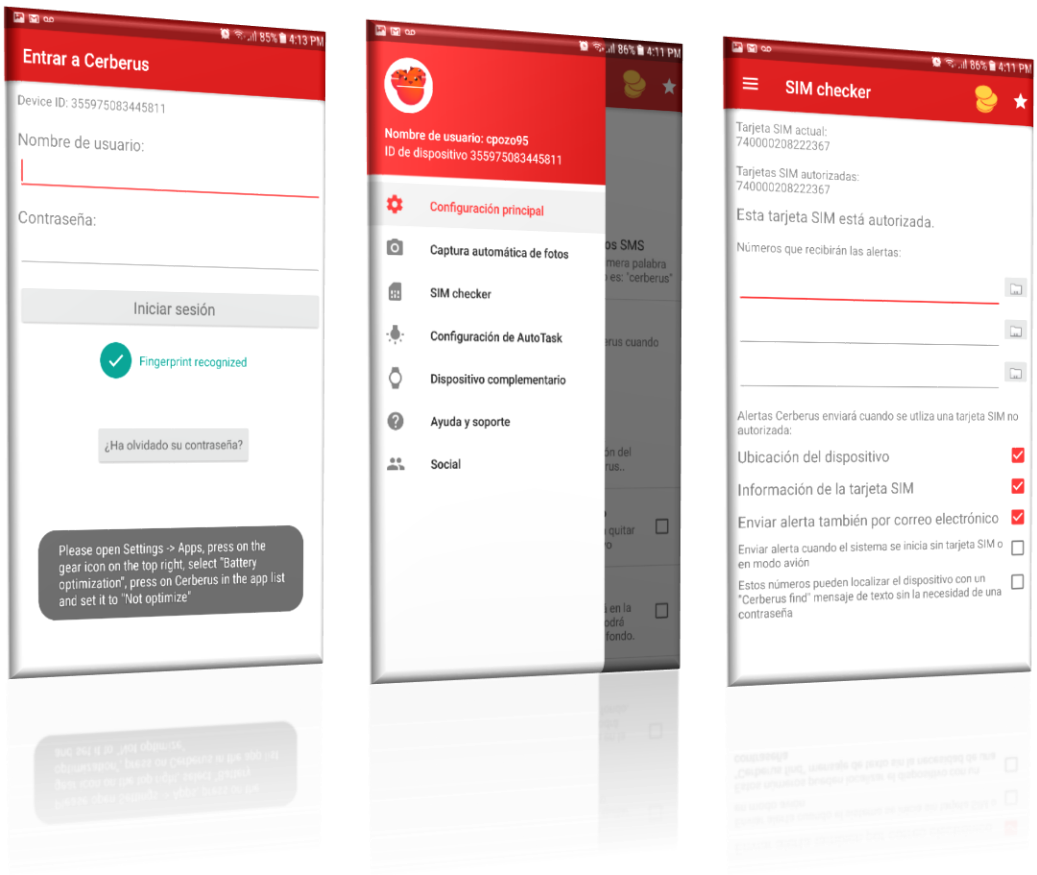

Ilustración 11: Pantallas Cerberus Anti Theft

Manejo

Luego de la instalación Cerberus solicita acceder a permisos de cámara para tomar fotografías y grabar vídeos, contactos, ubicación del dispositivo para rastreo, micrófono para grabar audio, realizar y administrar llamadas telefónicas, enviar y ver mensajes de SMS, imágenes, contenido multimedia y archivos del dispositivo. También solicita permisos para optimizar la batería y modificar configuraciones del sistema para una mayor confiabilidad.

La aplicación pregunta al usuario si ya tiene una cuenta registrada o si quiere crear una nueva. Al crear una cuenta nueva te pide ingresar usuario, contraseña y correo electrónico. Luego de aceptar los términos y condiciones se despliega un tutorial de cómo utilizar la aplicación y en la última pestaña pregunta al usuario si quiere dar acceso al administrador del dispositivo para poder realizar funciones de protección de desinstalar, borrado remoto y bloqueo con contraseña. Cuando se inicia sesión se despliega la configuración principal de Cerberus.

Características importantes

Tres formas de controlar el dispositivo:

- Control remoto a través de la web con la url: https://www.cerberusapp.com
- Control remoto vía SMS desde otro teléfono inteligente (la lista de comandos aplica de igual manera si es enviado por web)

  Man in the middle([Palabraclave][Contraseña][Comando]). Lista de comandos SMS disponibles:

  - Palabraclave contraseña find (Envía las coordenadas del dispositivo)
  - palabraclave contraseña siminfo (Información tarjeta SIM)
  - palabraclave contraseña lock código (Bloquear dispositivo mediante código, reemplazar *código*)
  - palabraclave contraseña unlock (Desbloque dispositivo)
  - palabraclave contraseña alarm texto (Muestra un mensaje sustituido por *texto* y reproduce una alarma fuerte)
  - palabraclave contraseña message texto (muestra un mensaje, sustituir *texto* con mensaje deseado)
  - palabraclave contraseña speak texto (dispositivo lee un mensaje, sustituir *texto* con mensaje deseado)
  - palabraclave contraseña call numero (para llamar a un teléfono, sustituir *numero* por un número telefónico)
  - palabraclave contraseña take picture (toma una fotografía y envía al correo electrónico establecido al crear la cuenta)
  - palabraclave contraseña capture video (graba un video y envía al correo electrónico establecido al crear la cuenta)
  - palabraclave contraseña screenshot (toma una captura de pantalla y envía al correo electrónico establecido al crear la cuenta)
  - palabraclave contraseña wipe (Borra memoria del dispositivo)
  - palabraclave contraseña wipe sd (Borra memoria de la tarjeta SD)
  - palabraclave contraseña start emergency horas (envía periódicamente información de la ubicación, sustituir *horas* con el número de horas a partir de una alerta a la siguiente)
  - palabraclave contraseña stop emergency (detiene el modo de emergencia)

- palabraclave contraseña enable data (activa conexión de datos móviles)
- palabraclave contraseña enable wifi (habilita el wifi y se conecta a cualquier red abierta automáticamente)
- palabraclave contraseña disable data (desactiva el acceso a datos móviles)
- palabraclave contraseña disable wifi (desactiva wifi)
- palabraclave contraseña enable roaming (habilitar el roaming de datos)
- palabraclave contraseña enable bluetooth (habilitar bluetooth)
- palabraclave contraseña disable bluetooth (deshabilitar bluetooth)
- palabraclave contraseña reboot (reinicia el dispositivo (solo funciona en teléfonos con acceso a root)

o Alertas Automáticas

- Ubicar los dispositivos en el mapa en la web y recibir coordenadas vía SMS
- Puede eliminar la información y guardar una copia de seguridad en la nube con Google Drive o Dropbox
- Si un usuario malintencionado tratar de ingresar una contraseña y falla, Cerberus realiza una captura fotográfica de la persona y lo envía al correo electrónico establecido al crear la cuenta por primera vez. Puede configurar el número de intentos fallidos
- Proteger administrador de dispositivo. Si el delincuente quiere desinstalar la aplicación, la aplicación fuerza al usuario a remover los privilegiados de administrador en la configuración del dispositivo, está función solicita una contraseña dificultando la desinstalación
- La función “FakeShutdown” engaña al usuario e imita cada acción de apagado del teléfono (como pantalla apagada y patrón de vibración desactivado)
- Otra característica es “Block Status Bar”. Como el delincuente puede acceder al menú de acceso rápido, incluso si el teléfono está bloqueado, la aplicación puede impedir acceso al bloquear cualquier funcionalidad relacionada con la barra de estado en un teléfono bloqueado

- Cerberus almacena el número de la tarjeta SIM al momento del registro de la aplicación. Si la tarjeta es removida SIM Checker enviaría una alerta con la información de la nueva tarjeta SIM y ubicación del dispositivo al número de teléfono registrado
- Configuración de Autotask. Cerberus permite configurar ciertos eventos como delimitar el dispositivo a cierta área del mapa. También podemos configurar ciertas condiciones, como el porcentaje de batería debajo del 15% y en todas estas situaciones podemos desencadenar algunas tareas. Las tareas pueden ser como tomar una fotografía o usar solo la cámara trasera, etc. Esta sección no tiene límite ya que el usuario puede usar su propia creatividad para diseñar diferentes eventos y sus correspondientes disparadores
- Soporte para Android Wear
- Modo incognito permite ocultar el icono de la aplicación
- Puede funcionar en combinación con la aplicación Cerberus Personal Safety que permite compartir la ubicación en tiempo real con cualquier familiar y/o amigos, creación de grupos para compartir a múltiples contactos, enviar mensaje personalizado, autorizar a personas confiables el acceder a mi ubicación en tiempo real cuando lo deseen, envió de mensajes a redes sociales, emails y contactos y creación de widget en pantalla de inicio (el funcionamiento depende del dispositivo)

Detalles anti-robo[a.20]

Esta tabla proporciona indicadores clave para medir funcionalidades de la aplicación en términos anti-robo dividido entre funcionalidades principales y secundarias. Entre otras cosas esta tabla trata de ayudar a los lectores a decidir si se beneficiaran de las características de seguridad más integrales y sofisticadas.

Ilustración 16: Detalles Anti-robo Cerberus Anti Theft

Detalles Anti-robo		
Características Principales		
Alarma		El ladrón no puede apagar la alarma durante 5 minutos, solamente si el dispositivo es desbloqueado
Borrado		Puede eliminar la memoria interna del teléfono incluyendo la tarjeta SD
Bloqueo		El código que se ingresa no tiene relevancia, el dispositibo se bloquea con el código del teléfono
Geolocalización		Sin internet no se puede localizar el dispositivo. Se visualiza el historial de las rutas en donde estuvo el dispositivo en el dashboard web
Mensajes		Envia un mensaje personalizado con la opción de reproducir verbalmente: Puede tener mensajes persistentes que no pueden ser eliminados y se desplegaran en la pantalla todo el tiempo.
Capturas de pantalla		No permite capturas de pantalla sin tener acceso root al dispositivo
Grabar pantalla		No permite grabar pantalla sin tener acceso root al dispositivo
Fotografías		Toma fotografías inmediatas en alta calidad con opción de usar la cámara trasera y flash
Grabar Videos		Permite grabar videos de hasta 30 segundo con opción usar la cámara trasera
Grabar Audio		Permite realizar grabaciones de hasta 5 minutos
Características Adicionales		
Modo Incognito		Permite ocultar la aplicación del menu, sin embargo requiere un reinicio
Forwarding		Todas las llamadas y mensajes no se envían a un número establecido
Multiplataforma		La app funciona para dispositivos Android exclusivamente. Móviles, Tablets, Phablets y SmartWatches
Dashboard Web		Se puede visualizar la ubicación del dispositivo en un mapa y enviar acciones a la aplicación
Envío de acciones		Se puede enviar acciones a la aplicación por Internet y por SMS
Activar/Desactiar Funciones		Permite deactivar y activar bluetooth, Wi-Fi, datos móviles, rastreo
Terminal de Android		Se puede enviar comandos especializados a traves del shell de Android
Obtener información del dispositivo		Despliega información de red, tarjeta SIM, redes Wi-Fi cercanas, aplicaciones instaladas, registro de llamadas y registro de mensajes
Modo Emergencia		Envía alertas periodicamente estableciendo el tiempo en horas
Fake Shutdown		No funciona el comando enviado por web
Iniciar Aplicación / Servicios		Con el nombre del paquete se puede iniciar aplicaciones y servicios remotamente
Copias de Seguridad		Permite almacenar mensajes, registro de llamas, videos, contactos y fotos. Se almacena en Google Drive y/o Dropbox

Ventajas

- La geolocalización es muy eficiente ya que almacena un historial de todas las ubicaciones en el dispositivo

- Puede guardar copias de seguridad en Google o en Dropbox asegurando información cuando se borra la tarjeta de memoria SD o la memoria del dispositivo interno

- La aplicación puede cambiar a modo incógnito y ocultarse rápidamente del menú de aplicaciones
- Cerberus dispone de varias herramientas que permiten rastrear al delincuente rápidamente. Se puede grabar videos, audios, tomar fotografías
- Permite el envío de acciones a través de SMS e internet
- Abrir aplicaciones y servicios enviando la acción mediante la web. Funcionalidad distinta a otras aplicaciones anti-robo
- Despliega información importante del dispositivo como el nombre de red a la cual está conectado, redes Wi-Fi cercanas, aplicaciones instaladas, registro de llamadas y de mensajes

Desventajas

- Solo se puede grabar y tomar capturas a la pantalla con acceso root
- La aplicación no permite el desvío de llamadas ni de mensajes
- El código de bloqueo para deshabilitar el uso del dispositivo no tiene relevancia, solamente bloquea el dispositivo con la contraseña predeterminada
- Interfaz poco amigable con el usuario y su diseño es solamente funcional
- El botón de apagado ficticio no es funcional. Tiene una interfaz poco creíble y puede ser evadida con facilidad mediante un hard reset

3.3. Prey: Open source theft recovery

Prey es un servicio freemium[31]que consta de un agente en sus dispositivos y un servicio web que maneja la información recopilada por el usuario. Está aplicación anti-robo permite rastrear y proteger tu teléfono inteligente extraviado o robado. Puedes gestionar y encontrar el dispositivo Android en una misma cuenta en un Panel Web. Realiza reportes sobre el dispositivo perdido como la ubicación, foto frontales y traseras, redes Wi-fi cercanas, etc ("Protección anti-robo para múltiples dispositivos | Prey", 2017).

[31] Freemium: Es un modelo de negocio que funciona ofreciendo servicios básicos gratuitos, mientras se cobra por otros más avanzados o especiales

La mayoría de las aplicaciones solo necesitan estar abiertas desde el dispositivo y se ejecutarán. Prey es distinto. Mientras la aplicación se ejecuta en el dispositivo, el usuario es quien administra todo desde su Panel de control. Puede activar todas las acciones, la ubicación y los informes desde un solo lugar.[a.21][CP22]

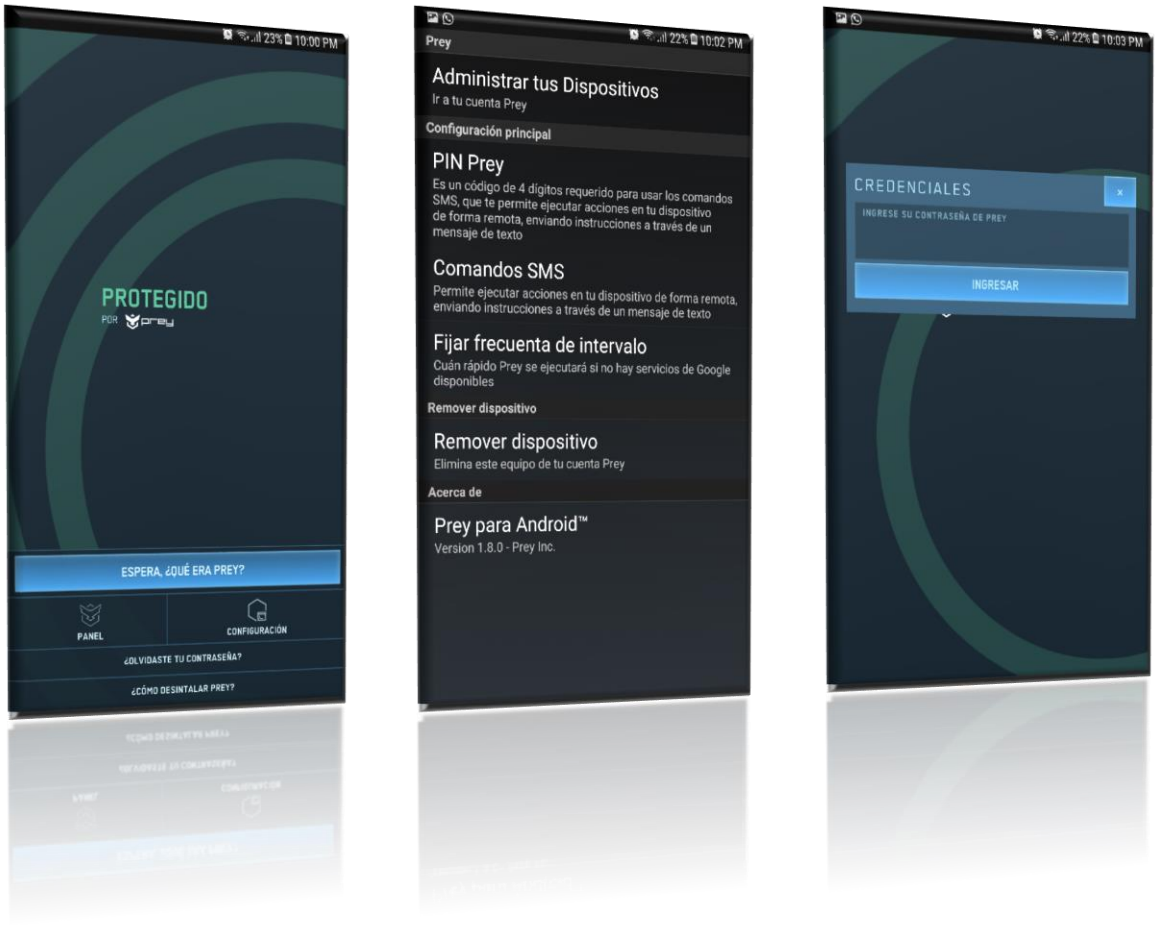

Ilustración 12: Pantallas Prey Anti Theft

Manejo

Al instalar la aplicación se inicia una interfaz gráfica que contiene una guía de qué es Prey y como desinstalarlo, panel de control, configuraciones, solicitar permisos y recuperar contraseña. Prey solicita permisos de cámara, ubicación, administración de llamas telefónicas y acceder al contenido multimedia del dispositivo.

Al ingresar en configuraciones se despliega la administración de la cuenta (direccionamiento web) y una lista de configuraciones principales. La primera es el PIN que se requiere configurar al enviar comandos SMS, la segunda activa y desactiva los comandos SMS e indica cuales son,

la tercera permite fijar la frecuencia de ejecución de Prey si los servicios de Google no están disponibles y la cuarta remueve la cuenta del equipo actual.

Características importantes

- Módulo de registro y manejo de usuarios mediante redes sociales (Facebook/Twitter)
- Cuenta con el modo profesional y el básico
- Geolocalización de dispositivos en mapa de tiempo real
- Bloquear el dispositivo después del robo
- Eliminar remotamente todos los datos confidenciales de una computadora de trabajo, teléfono o tablet.
- Territorios limitados en el mapa (Control Zones)
- Recuperación de datos
- Enviar distintos tipos de alarma al dispositivo
- Gestión de varios dispositivos al mismo tiempo
- Restaurar a los valores predeterminados de fábrica un dispositivo Android
- Supervisa los cambios de hardware
- Recopila información de los dispositivos a lo largo del tiempo a medida que los informes

Detalles anti-robo[a.23]

Esta tabla proporciona indicadores clave para medir funcionalidades de la aplicación en términos anti-robo dividido entre funcionalidades principales y secundarias. Entre otras cosas esta tabla trata de ayudar a los lectores a decidir si se beneficiaran de las características de seguridad más integrales y sofisticadas.

Tabla 3: Resultados Prey Anti Theft

Detalles Anti-robo		
Características Principales		
Alarma		El ladrón puede apagar el dispositivo para terminar el sonido
Borrado		El dispositivo restablece los valores predeterminados de fábrica. Tarjeta SD incluida.
Bloqueo		Si se aplica un hard reset el dispositivo deja de bloquearse momentaneamente
Geolocalización		Sin internet no se puede localizar el dispositivo. Se visualiza el historial de las rutas en donde estuvo el dispositivo en el dashboard web
Mensajes		Envia un mensaje personalizado. Desaparece en segundos
Capturas de pantalla		No permite capturas de pantalla
Grabar pantalla		No permite grabar pantalla
Fotografías		Toma fotografías automaticamente cuando el estado del dispositivo cambia a perdido
Grabar Videos		No permite grabar videos
Grabar Audio		No permite realizar grabaciones
Características Adicionales		
Modo Incognito		Permite ocultar la aplicación del menu rapidamente
Forwarding		Todas las llamadas y mensajes no se envían a un número establecido
Multiplataforma		La app funciona para dispositivos Android, IOS. Móviles, Tablets, Phablets,PC y SmartWatches
Dashboard Web		Se puede visualizar la ubicación del dispositivo en un mapa y enviar acciones a la aplicación
Envío de acciones		Se puede enviar acciones a la aplicación por Internet y por SMS
Activar/Desactiar Funciones		No permite deactivar y activar bluetooth, Wi-Fi, datos móviles, rastreo
Terminal de Android		No permite enviar comandos especializados a traves del shell de Android
Obtener información del dispositivo		Despliega información solamente del hardware del dispositivo
Modo Emergencia		Envía alertas periodicamente estableciendo el tiempo en horas
Fake Shutdown		No permite simular el botón de apagado
Iniciar Aplicación / Servicios		Con el nombre del paquete se puede iniciar aplicaciones y servicios remotamente
Copias de Seguridad		Permite almacenar mensajes, registro de llamas, videos, contactos y fotos. Se almacena en Google Drive y/o Dropbox

Ventajas

- Es una de las pocas aplicaciones anti-robo de código abierto
- Las acciones pueden ser ejecutadas por comando SMS si la necesidad de estar conectado a Internet
- Prey puede camuflarse entrando en modo incognito en el menú de aplicaciones
- Prey tiene a su disposición una lista de acciones rápidas y prácticas al momento de una emergencia

- Web dashboard para manejar la geolocalización y las acciones disponibles conectado a través de un servicio web con el dispositivo Android
- Puede monitorear y agrupar múltiples dispositivos al mismo tiempo. Ideal para empresas y gerentes de TI
- Puede eliminar todos los archivos y recuperar la información deseada enviando un link de descarga al correo electrónico
- La aplicación tiene licencia GNU (GENERAL PUBLIC LICENSE) versión 3, 29 de junio del 2007

Desventajas

- Si el sistema operativo se remueve del dispositivo la aplicación se elimina
- No hay forma de controlar un dispositivo si no se envían datos, por lo que es vital que esté encendido y conectado a internet. Sin embargo, es el requisito mínimo que cualquier agente similar necesita
- No hay forma de rastrear el dispositivo con el número de teléfono, número de serie, IMEI u otros. Esta información no proporciona una ubicación y el dispositivo no podría conectarse con los servidores Prey. Además, podría entrar en conflicto con las leyes sobre espionaje y privacidad
- No permite tomar capturas de pantalla, grabar videos y audios en el dispositivo
- No soporta la activación y desactivación remota de las funciones del teléfono

3.4. Avast Anti-Theft

Avast es una aplicación con más de 100 millones de instalaciones que centra sus capacidades en proteger al dispositivo contra los ciberataques y robos personales. Nos centraremos en las funcionalidades anti-robo que requieren un pago y mantienen un estado de prueba de 15 días.

Avast permite al usuario tener una comunicación permanente con múltiples dispositivos mediante su administrador web y mensajes SMS. Contiene múltiples opciones para encontrar tu dispositivo entre las más importantes están en geolocalización, captura de contenido multimedia, bloqueo del dispositivo y respaldo en Google Drive.

No obstante, su código fuente no es abierto para el público y está [a.24]protegido por leyes de propiedad intelectual en los Estados Unidos.

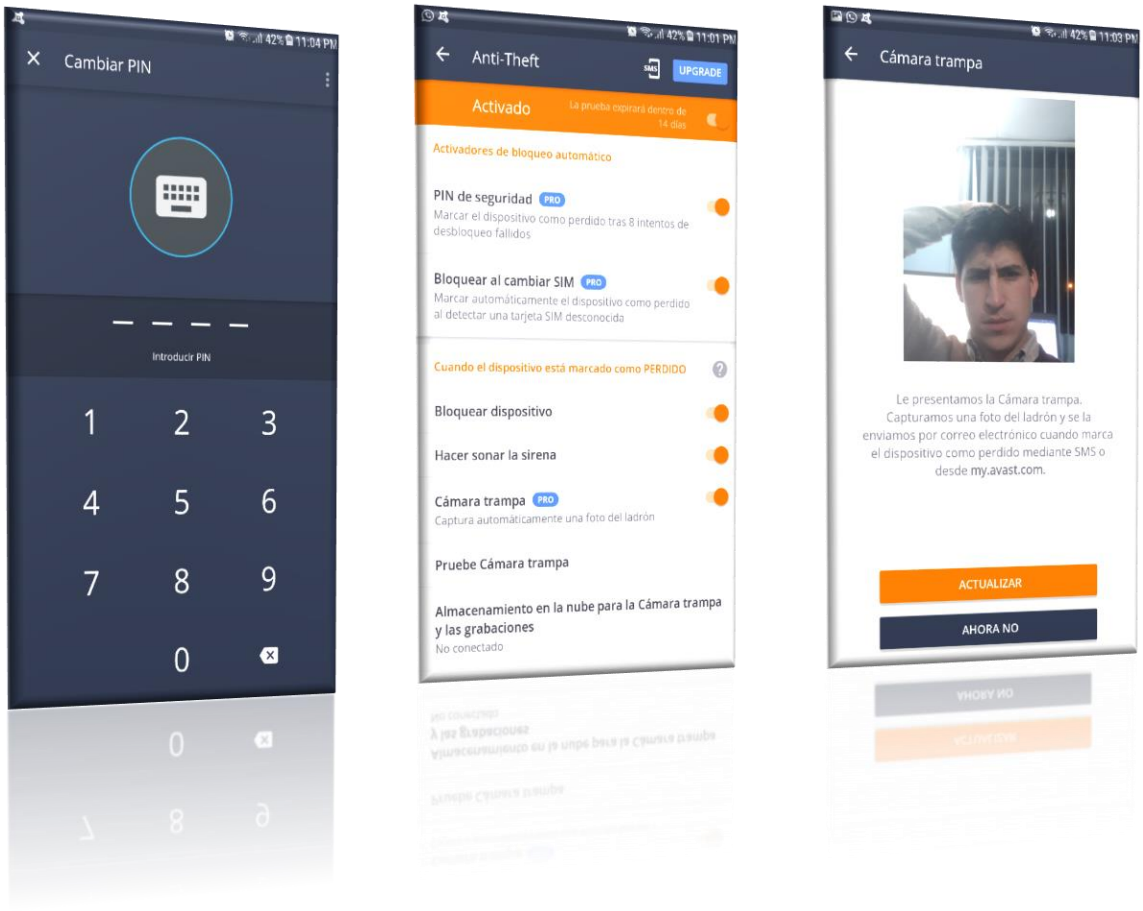

Ilustración 13: Pantallas Avast Anti-Theft

Manejo

Al instalar la aplicación Ingresamos al menú de opciones y presionamos la opción “anti theft” que despliega todas las configuraciones anti-robo de la aplicación. Para activar las funcionalidades anti- robo se requieren 3 sencillos pasos.

1. Establecer un pin y una cuenta para asociarla a la aplicación, para realizar estos pasos se requiere la autenticación del propio dispositivo
2. Solicitar la creación de una cuenta en Avast o conectar a través de redes sociales (Google+ y Facebook) para acceder al administrador web
3. Conceder permisos de administrador al dispositivo para poder bloquear de forma remota el dispositivo inmediatamente o borrar sus datos.

Características importantes

- Para obtener funcionalidades extras de se requiere actualiza la cuenta a Avast Mobile Security Pro. La actualización incluye eliminación de anuncios, bloqueo de aplicaciones, cámara trampa, seguridad SIM, almacén de fotos, última ubicación conocida, soporte directo
- Administrador web para controlar todos los dispositivos que tengan instalado Avast Anti theft
- Cuando se marca el dispositivo como perdido, Avast Anti-Theft automáticamente toma una foto del posible ladrón y graba un archivo de audio para ubicar el dispositivo. Si selecciona Google Drive en la sección de almacenamiento de la nube, la foto y el archivo de audio grabado se envían a Google Drive.
- Geolocalización del dispositivo mediante mapas térmicos y reportes sobre el historial de ubicación
- La opción Marcar como perdido cambia el estado del dispositivo e involucra un conjunto de acciones como enviar alarmas y bloquear el dispositivo
- Proporciona información detallada del dispositivo, estado de la batería actual, IMEI, la última comunicación con el dispositivo, red, etc[a.25].
- Desviar llamadas y mensajes SMS a otro número de teléfono con copia a cualquier teléfono
- Control remoto a través de SMS y bloquear teléfono al cambiar tarjeta SIM
- Acciones de borrado, grabar audio, fotografías, obtener datos (llamadas, contactos, sms) y contactar con mensajes y llamadas ocultas para escuchar lo que sucede alrededor del dispositivo
- Contactarse con el usuario malintencionado a través de mensajes y llamadas

Detalles anti-robo[a.26]

Esta tabla proporciona indicadores clave para medir funcionalidades de la aplicación en términos anti-robo dividido entre funcionalidades principales y secundarias. Entre otras cosas esta tabla trata de ayudar a los lectores a decidir si se beneficiarán de las características de seguridad más integrales y sofisticadas.

Tabla4: Pantallas Avast Anti-Theft

Detalles Anti-robo		
Características Principales		
Alarma		Se envía una alarma comentando que el dispositivo ha sido robado o extraviado
Borrado		Elimna por completo la lista de contactos, registro de llamadas, SMS / MMS, historial del navegador, aplicaciones y cuentas de correo electrónico
Bloqueo		El dispositivo se bloquea automaticamente aunque se reinicie
Geolocalización		Sin internet no se puede localizar el dispositivo. Se visualiza el historial de las rutas en donde estuvo el dispositivo en el dashboard web
Mensajes		Envia un mensaje personalizado. Puede eliminarse facilmente
Capturas de pantalla		No permite capturas de pantalla
Grabar pantalla		No permite grabar pantalla
Fotografías		Toma fotografías inmediatas con opción de usar la cámara trasera y reconocimiento facial
Grabar Videos		No permite grabar videos
Grabar Audio		Permite realizar grabaciones de hasta 5 minutos
Características Adicionales		
Modo Incognito		Permite ocultar la aplicación del menu, sin embargo requiere un reinicio
Forwarding		Todas las llamadas y mensajes se envían a un número establecido
Multiplataforma		La app funciona para dispositivos Android e IOS Móviles, Tablets, Phablets y SmartWatches
Dashboard Web		Se puede visualizar la ubicación del dispositivo en un mapa y enviar acciones a la aplicación
Envío de acciones		Se puede enviar acciones a la aplicación por Internet y por SMS
Activar/Desactiar Funciones		Permite deactivar y activar bluetooth, Wi-Fi, datos móviles, rastreo
Terminal de Android		Se puede enviar comandos especializados a traves del shell de Android
Obtener información del dispositivo		Despliega información del sistema operativo, de los productos Avast instalados, versión del SDK, operador móvil, nombre del dueño, estado de bateria, comunicación entre la weby el dispositivo, etc.
Modo Emergencia		Envía múltiple acciones dependiendo de las configuraciones: Geolocalización, Bloquear, Sirena, etc.
Fake Shutdown		No funciona el comando enviado por web
Iniciar Aplicación / Servicios		Con el nombre del paquete se puede iniciar aplicaciones y servicios remotamente
Copias de Seguridad		Permite almacenar mensajes, registro de llamadas y contactos

Ventajas

- Avast Anti-theft permite al usuario probar las funcionalidades pagadas por 15 días para comprobar que el usuario este conforme con el pago
- La funcionalidad de alarma activa el volumen a su máxima capacidad y reproduce una voz pronunciando que el dispositivo está perdido o fue robado llamando la atención del público

- Su interfaz es muy intuitiva y sencilla de utilizar. La experiencia del usuario es meticulosamente pensada en la aplicación. Se puede apreciar diseño UX/UI en la aplicación
- Redirige las llamadas y mensajes del usuario malintencionado a número de teléfono preferido. Una funcionalidad muy efectiva y que pocas aplicaciones utilizan
- Historial de comandos y configuraciones activadas para el envió de acciones

Desventajas

- Para obtener buenos resultados y funcionalidades importantes es necesario actualizar la cuenta al plan Avast Mobile Security Pro
- El modo incognito no esconde la aplicación en el menú de navegación del dispositivo móvil
- No permite muchas funcionalidades que la industria de software anti-robo permite como estándar. No permite grabar videos, capturar y grabar pantallas y el modo incognito no es funcional
- Activar o desactivar funciones como Wifi o bluetooth no está permitido en la aplicación

3.5. Where'smyDroid

Wheres's my Droid es la primera aplicación anti-robo en el mercado digital de Android, creada por la start-up Alienman Technologies, lleva un tiempo en el mercado. Lanzamiento oficial mayo, 2009.Provee al usuario funcionalidades primordiales como geolocalización, envió de mensajes, modo incógnito, etc. y funciones avanzadas como borrar memoria, tomar fotografías, bloquear dispositivo.

El uso de funcionalidades depende del plan contratado. Existen 3 planes:

- Gratuito: Ubicación GPS, llamada de GPS por batería baja, alarma, contraseña para acceder al administrador, alarma al remover tarjeta sim y permisos de envió de comandos a través de mensajes
- Pro $3,99s: Cámara y tomar fotografía al fallar desbloqueo, bloquear pantalla remotamente, wipe tarjeta SD y realizar un reseteo de fábrica, esconder icono, prevenir desinstalación y disponible para un solo dispositivo

- Elite 0,99/mes: Geofence (Perímetro autorizado), alertas anti-robo, actualiza ubicación constantemente, visualizar lista de contactos y registro de llamadas, visualizar redes wifi cercanas y disponible para múltiples dispositivos

Su modelo de negocios se basa en anuncios en el plan gratuito y en suscripciones mensuales en el plan Pro y Elite. Where's my Droid es una aplicación exclusiva para dispositivos Android debido a las restricciones de seguridad del sistema operativo IOS.

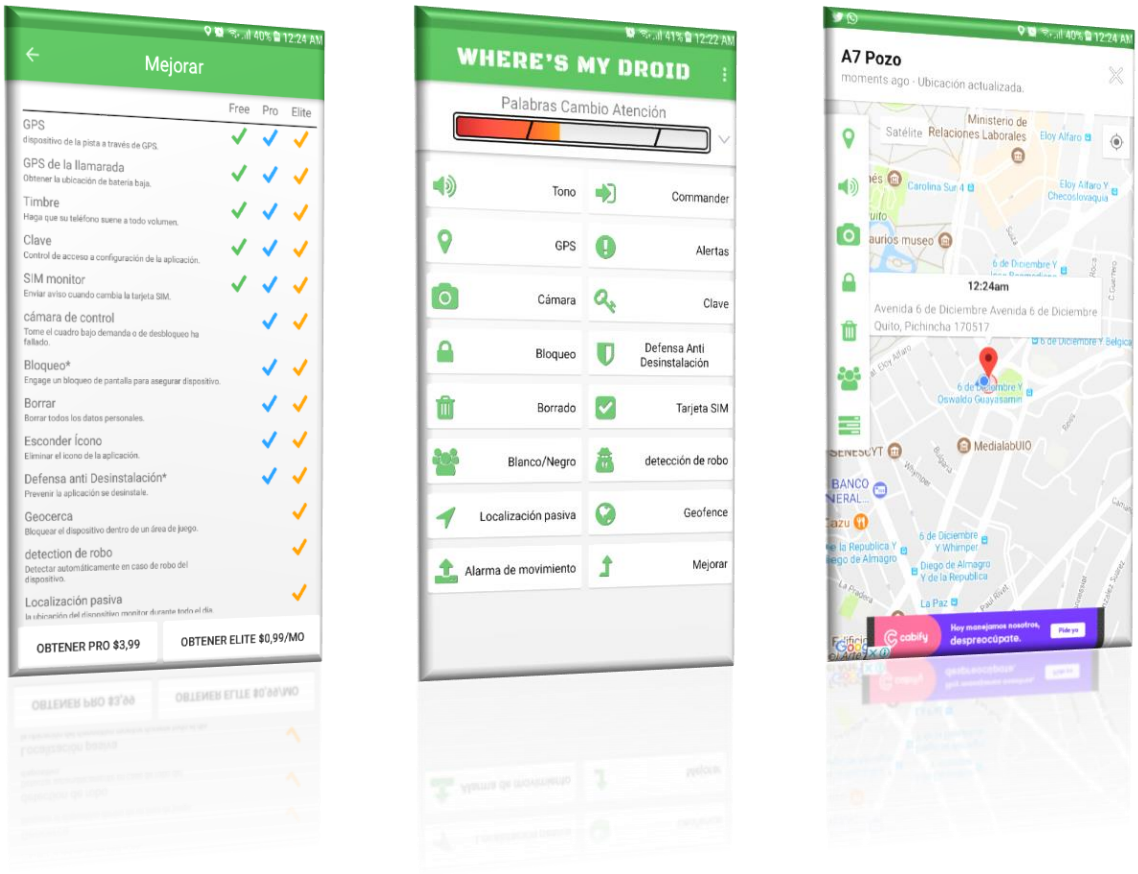

Ilustración 14: Pantallas Where'smyDroid

Manejo

Finalizada la instalación de la aplicación se despliega una pantalla solicitando al usuario iniciar la configuración. El primer paso es aceptar los términos y condiciones. La segunda pantalla solicita al usuario permisos, entre estos la ubicación, SMS, teléfono y contactos, por último, el uso de la cámara. La creación de una cuenta es necesaria para ingresar al administrador de la aplicación.

Al ingresar al administrador de la aplicación se requiere activar el resto de los permisos para activar todas sus funcionalidades. Al activar todos los permisos se despliega una barra en la parte superior que guía al usuario para configurar toda la aplicación con todas las medidas de seguridad. En la parte central de la pantalla del administrador se encuentran todas las acciones anti-robo que podemos realizar.

Características importantes

- La aplicación permite configurar los comandos SMS para enviar acciones al dispositivo desde otro teléfono
- Tiene un administrador web
- Características de GPS, geolocalización
- Disparador que envía ubicación del dispositivo al tener poca batería
- Al ejecutar el comando alarma sube el volumen del dispositivo al máximo
- Proteja la configuración de la aplicación para que no se modifique
- Siempre alerta de las modificaciones de la tarjeta SIM
- Controla permisos para enviar comandos vía SMS
- Toma fotografías por demanda y al fallar desbloqueando el dispositivo
- Bloqueo remoto para prevenir acceso no autorizado
- Eliminar todos los datos personales del dispositivo
- Aplicación detecta patrones de robo y cambia de estado puede bloquear pantalla, enviar correo, etc.
- Actualiza automáticamente la ubicación del dispositivo a lo largo del día
- Almacena el historial de ubicaciones de tu dispositivo
- Remotamente descarga contactos y registro de llamadas
- Consultar estadísticas sobre el dispositivo, como nivel de batería y si el GPS está habilitado
- Ver redes wifi disponibles en el área

Detalles anti-robo

Esta tabla proporciona indicadores clave para medir funcionalidades de la aplicación en términos anti-robo dividido entre funcionalidades principales y secundarias. Entre otras cosas esta tabla trata de ayudar a los lectores a decidir si se beneficiaran de las características de seguridad más integrales y sofisticadas.

Tabla 5: Resultados Where'smyDroid

Detalles Anti-robo		
Características Principales		
Alarma		Se envía una alarma comentando que el dispositivo ha sido extraviado. Múltiples configuraciones entre estas utilizar flash, tono personalizado, duración de alarma, etc.
Borrado		Elimina la información del dispositivo reestableciendolo al modo fábrica con la opción de eliminar la tarjeta SD
Bloqueo		El dispositivo se bloquea automaticamente confgurando un PIN para prevenir acceso no autorizado
Geolocalización		Sin internet no se puede localizar el dispositivo. Se visualiza el historial de las rutas en donde estuvo el dispositivo en el dashboard web
Mensajes		No permite el envio de mensajes personalizados
Capturas de pantalla		No permite capturas de pantalla
Grabar pantalla		No permite grabar pantalla
Fotografías		Toma fotografías inmediatas con opción de usar la cámara trasera y flash
Grabar Videos		No permite grabar videos
Grabar Audio		No permite realizar grabaciones de audio
Características Adicionales		
Modo Incognito		Ocultar el ícono de la aplicación desde la pantalla de inicio
Forwarding		No permite desviar Todas las llamadas y mensajes hacia un número de teléfono establecido
Multiplataforma		La app funciona para dispositivos Android Móviles, Tablets, Phablets y SmartWatches
Dashboard Web		Se puede visualizar la ubicación del dispositivo en un mapa y enviar acciones a la aplicación
Envío de acciones		Se puede enviar acciones a la aplicación por Internet y por SMS
Activar/Desactiar Funciones		Permite deactivar y activar la aplicación llamando desde otra línea previamente configurado en una lista. No permite activar otras funciones.
Terminal de Android		Se puede enviar comandos especializados a traves del shell de Android
Obtener información del dispositivo		Despliega estadísticas sobre su dispositivo, como el nivel de la batería y si el GPS está habilitado.
Modo Emergencia		Envía múltiple acciones dependiendo de las configuraciones: Geolocalización, Bloquear, Sirena, etc.
Fake Shutdown		No funciona el comando enviado por web
Iniciar Aplicación / Servicios		Con el nombre del paquete se puede iniciar aplicaciones y servicios remotamente
Copias de Seguridad		Solo permite descargar contactos y registro de llamadas

Ventajas

- Conoce las necesidades del mercado más tiempo que sus competidores
- Funciones principales mucho más robustas
- Modo incognito efectivo. No permite desinstalar la aplicación y oculta el icono de la pantalla de aplicaciones

Desventajas

- La aplicación prioriza anuncios en su versión gratuita. No permite utilizar la aplicación hasta que el anuncio finalice
- Funcionalidades principales se obtienen con los planes de pago más avanzados
- La aplicación está compuesta por funcionalidades muy pragmáticas para el usuario sin embargo su interfaz no fue orientada alDiseño UX (Experiencia de Usuario)
- Limitación de característica adicionales como grabar videos, audio, forwarding[32]etc.

3.6. Análisis Comparativo

Una vez expuestos los resultados de las aplicaciones anti-robo más importantes en el mercado, se presenta a continuación un análisis comparativo entre las cinco aplicaciones. Este tipo de análisis permite determinar si existen diferenciassignificativas entre las diferentes aplicaciones, que conduzcan a conclusiones objetivas.

[32]Forwarding: Es la acción de redirigir un puerto de red de un nodo de red a otro

Tabla 6: Resumen Puntuación

Aplicaciones Anti-Robo	Encontrar mi Dispositivo	Prey Anti-Theft	Cerberus Anti Theft	Avast Anti-Theft	Where's My Droid
Alarma					
Borrado					
Bloqueo					
Geolocalización					
Mensajes					
Capturas de pantalla					
Grabar pantalla					
Fotografías					
Grabar Videos					
Grabar Audio					
Características Adicionales					
Modo Incognito					
Forwarding					
Multiplataforma					
Dashboard Web					
Envío de acciones					
Activar/Desactiar Funciones					
Terminal de Android					
Obtener información del dispositivo					
Modo Emergencia					
Fake Shutdown					
Iniciar Aplicación / Servicios					
Copias de Seguridad					

4. Capítulo IV: Evaluación de funcionalidades en aplicaciones anti-robo utilizando dispositivo Android

La evaluación de funcionalidades brinda al lector un entendimiento profundo de cada característica anti-robo, para entender la efectividad, usabilidad y dificultad de cada función. Se utilizó un método de evaluación personalizado con el objetivo de evaluar y analizar varios factores. El método está compuesto por varias etapas, estas son:

- Análisis de fases: Clasificación de funcionalidades. Se analizan todas las etapas de la funcionalidad, esto es antes, durante y después del robo

- Análisis de efectividad: Utilizando la clasificación previa del análisis de fases evaluamos la efectividad de la función y si requiere de otras funcionalidades para actuar efectivamente. De acuerdo con el método se identifican las variables que pueden medirse: confiabilidad, funcionalidad, portabilidad, usabilidad, eficiencia y mantención

- Servicio de terceros: Que servicios de terceros utiliza y con cuales funcionalidades se integran

- Mejora de funcionalidades: Se clasifica en 3 partes factibilidad, deseabilidad y viabilidad

Una vez definidos los atributos, métricas y valores se proceden a realizar la evaluación por cada sub-atributo que compone los criterios a evaluar. Ese resultado permite identificar las fortalezas y debilidades de las funcionalidades auditadas y de esa manera orientar la observación a esclarecer las causas que ocasionan la baja puntuación

4.1 Análisis de Fase

La clasificación de funcionalidades es esencial para entender el flujo que recorre cada función individual y organizarlas en una misma estructura para su posterior evaluación de efectividad.

Existen 3 etapas:

- Antes del robo: El dispositivo se encuentra con su propietario y no ha sufrido ninguna modificación

- Durante el robo: El delincuente posee el dispositivo un corto periodo y fue removido del propietario ese instante
- Después del robo: El delincuente posee el dispositivo un largo periodo

Clasificación funcionalidades

- Alarma
    - Antes: No funcional
    - Durante: Al extraviar el dispositivo se envía un comando para emitir un sonido de preferencia durante un tiempo determinado. Es funcional si el dispositivo se encuentra a 10 metros
    - Después: No funcional

- Borrado
    - Antes: No funcional
    - Durante: El momento del robo el usuario puede eliminar toda la información de la tarjeta SD y memoria interna del teléfono
    - Después: Si el robo a ocurrido el usuario debe revisar si existe comunicación con el dispositivo y enviar el comando wipe data

- Bloqueo
    - Antes: No funcional
    - Durante: Protege la información del usuario bloqueando el dispositivo mediante un código establecido por el propietario
    - Después: Si existe comunicación con el dispositivo puede bloquearse

- Geolocalización
    - Antes: No funcional
    - Durante: Localiza tu dispositivo rápidamente durante el robo
    - Después: Si existe comunicación con el dispositivo se puede ubicar incluso después de días

- Mensajes
    - Antes: No funcional

  - Durante: Envía mensajes durante el robo
  - Después: Envía mensajes después del robo

- Capturas de pantalla
  - Antes: No funcional
  - Durante: Visualizar que hace el delincuente, sin embargo, durante el robo es improbable que el delincuente manipule el dispositivo
  - Después: En esta etapa el delincuente manipula el dispositivo y el usuario puede visualizar sus acciones mediante capturas de pantalla

- Grabar pantalla
  - Antes: No funcional
  - Durante: Visualizar que hace el delincuente, sin embargo, durante el robo es improbable que el delincuente manipule el dispositivo
  - Después:En esta etapa el delincuente manipula el dispositivo y el usuario puede visualizar sus acciones grabando la pantalla

- Fotografías
  - Antes: No funcional
  - Durante: Permite tomar fotografías al delincuente durante el robo
  - Después: Si existe comunicación con el dispositivo se puede tomar fotografías del delincuente después del robo o ver el entorno en el que se encuentra el dispositivo

- Grabar videos
  - Antes: No funcional
  - Durante: Permite grabar videos del delincuente durante el robo
  - Después: Si existe comunicación con el dispositivo se puede grabar al delincuente después del robo o ver el entorno en el que se encuentra el dispositivo

- Grabar audio
  - Antes: No funcional
  - Durante: Permite grabar audios del dispositivo durante el robo

  - Después: Durante el robo se puede grabar el audio del delincuente. Puede servir como prueba si el usuario establece juicio

- Modo incógnito
  - Antes: Se configura antes del robo
  - Durante: La primera acción probable es deshacerse de cualquier aplicación que comunique al usuario, esto es aplicaciones anti-robo y antivirus. Si no se activa previo al robo no tiene funcionalidad
  - Después: Si no se activa previo al robo no tiene funcionalidad

- Forwarding
  - Antes: Se requiere configuración previa al robo
  - Durante: No funcional
  - Después: Permite comunicarse con el delincuente forzadamente

- Activar/desactivar funciones
  - Antes: No funcional
  - Durante: Activar funciones durante el robo permite al usuario obtener una ventaja estratégica sobre el delincuente
  - Después: Obtener información coherente y precisa utilizando distintas funciones del dispositivo

- Terminal de Android
  - Antes: No funcional
  - Durante: No funcional
  - Después: El usuario puede ejecutar funciones específicas y más avanzadas, esto requiere tiempo y es funcional a largo plazo

- Obtener información del dispositivo
  - Antes: Permite obtener información del dispositivo
  - Durante: Visualizar el estado de la batería o a que red wifi está conectado
  - Después: Funcional a largo plazo

- Modo emergencia

- Antes: No funcional
- Durante: Activa y ejecuta funciones sin la autorización del usuario. Funcional para situaciones críticas
- Después: No funcional

- Fakeshutdown
  - Antes: Configurar previo a la emergencia
  - Durante: Funcional si el delincuente trata de apagar el dispositivo, se activa una notificación y se apaga la pantalla
  - Después: No funcional

- Iniciar aplicaciones/servicios
  - Antes: No funcional
  - Durante: No funcional
  - Después: El usuario puede accionar funciones o aplicaciones, esto requiere tiempo y es funcional a largo plazo

- Copias de seguridad
  - Antes: El usuario puede realizar una copia para prevenir cualquier emergencia
  - Durante: Si el delincuente no termina la comunicación o apaga el dispositivo la copia de seguridad puede ejecutarse
  - Después: No funcional, los datos fueron expuestos a largo plazo

Tabla 7: Clasificación Funcionalidades

Clasificación Funcionalidades	Antes	Durante	Después
Alarma		✓	
Borrado		✓	✓
Bloqueo		✓	✓
Geolocalización		✓	✓
Mensajes		✓	✓
Capturas de Pantalla		✓	✓
Grabar Pantalla		✓	✓
Fotografías		✓	✓
Grabar Videos		✓	✓
Grabar Audio		✓	✓

Modo Incógnito	✓	✓	✓
Forwarding	✓		✓
Activar/Desactivar Funciones		✓	✓
Terminal Android			✓
Obtener Información	✓	✓	✓
Modo Emergencia		✓	
FakeShutdown	✓	✓	
Iniciar aplicaciones/servicios			✓
Copias de Seguridad	✓	✓	✓

4.2 Análisis de métricas

De acuerdo con el método de evaluación se identifican las variables que pueden medirse: Confiabilidad, funcionalidad, usabilidad y eficiencia descritas como sigue:

- Confiabilidad

Habilidad de la función para mantenerse operativo (funcionando). En alguna medida representa el grado de seguridad con que funcione sin ser detectado por el delincuente.

- Funcionalidad

Habilidad de la función para realizar el trabajo deseado. Capacidad de la función para proveer las características que satisfacen las necesidades explícitas e implícitas cuando el dispositivo se utiliza bajo condiciones específicas.

- Usabilidad

Capacidad de la función de ser entendido, aprendido y usado en forma fácil y atractiva. Debe tener una interfaz de usuario apropiada y una documentación adecuada.

- Eficiencia

Es la forma del desempeño adecuado de la función. No debe hacer que se malgasten el tiempo del usuario y debe obtener el mayor beneficio dependiendo la función.

Tabla 8: Niveles o Escalas

Valores	Puntaje
Deficiente	1
Insuficiente	2
Aceptable	3
Sobresaliente	4

Alarma

- Confiabilidad: Funciona con precisión al momento de activarla sin ser detectada por el delincuente. Su confiabilidad depende en gran medida del modo incognito, por esa razón la función es sobresaliente

- Funcionalidad: Es insuficiente, en escenarios reales no puede servir como un método anti-robo. En escenarios poco probables puede aplicar por esta razón la función es insuficiente

- Usabilidad: La función no requiere ninguna entrada y es sencilla operarla. Sin embargo, la complejidad de la interfaz puede cambiar dependiendo de la aplicación, por esa razón la función es sobresaliente

- Eficiencia: Es una función simple y precisa, no requiere de cálculos ni de instrucciones complejas. Envía un comando a través de la red y la aplicación lo interpreta por esta razón la función es sobresaliente

Borrado

- Confiabilidad: Funciona con precisión al momento de activarla sin ser detectada por el delincuente. Su confiabilidad depende en gran medida del modo incognito por esa razón la función es sobresaliente

- Funcionalidad: Es aceptable en muchos escenarios. Sin embargo, el usuario tiene que reaccionar rápido ya que el delincuente puede deshabilitar la conexión o apagar el dispositivo. Dependiendo de la aplicación los datos pueden permanecer en el dispositivo por esta razón la función es insuficiente

- Usabilidad: La función requiere de algunas configuraciones de borrado y esto puede confundir al usuario. El usuario desconoce que se elimina del dispositivo, por esta razón la función es insuficiente

- Eficiencia: Requiere de una conexión activa y constante, los tiempos depende de la aplicación. Sin embargo, la mayoría tarda en eliminar todos los datos del dispositivo y en algunas ocasiones no elimina todos los datos necesarios, por esta razón la función es insuficiente

Bloqueo

- Confiabilidad: Puede activarse sin que el delincuente lo detecte. No obstante, el delincuente puede apagar el dispositivo inhabilitando cualquier acción del usuario por esta razón la función es aceptable

- Funcionalidad: En situaciones de emergencia el dispositivo queda completamente bloqueado y no permite realizar ninguna acción al delincuente mas que apagar el dispositivo para impedir acciones, por esta razón la función es sobresaliente

- Usabilidad: La función no requiere ninguna entrada y es sencilla operarla. Sin embargo, la complejidad de la interfaz puede cambiar dependiendo de la aplicación, por esa la función es sobresaliente

- Eficiencia: El usuario ejecuta el comando y en poco tiempo se bloquea el dispositivo. Su velocidad dependerá de la conexión de red, por esa razón la función es sobresaliente

Geolocalización

- Confiabilidad: Se activa automáticamente y se actualiza constantemente en segundo plano. Su confiabilidad depende en gran medida del modo incognito por esa razón la función es sobresaliente

- Funcionalidad: Si el dispositivo se queda sin conexión a internet, la geolocalización se anula. Funciona bien en escenarios donde el delincuente no remueve la conexión ni apaga el dispositivo, por esta razón la función es aceptable

- Usabilidad: La configuración es sencilla, en algunos casos preconfigurada. Se ejecuta automáticamente sin la necesidad del usuario. Dependiendo del teléfono la precisión puede fallar por esta razón la función es sobresaliente

- Eficiencia: El usuario obtiene las coordenadas rápidamente. Sin embargo, puede tener retrasos dependiendo la conexión de red, por esta razón la función es sobresaliente

Mensajes

- Confiabilidad: Su característica principal es alertar al ladrón. Sin embargo, mientras exista conexión de red con el dispositivo su operatividad no se verá afectada en lo absoluto, por esta razón la función es sobresaliente

- Funcionalidad: En escenarios donde el dispositivo ha sido robado, muchas veces enviar un mensaje al delincuente no es del todo útil y puede alertarlo de que alguna

aplicación anti-robo se encuentra instalada en el dispositivo, por esta razón la función es insuficiente

- Usabilidad: La función solicita una entrada donde el usuario escribe el mensaje y presiona enviar. La complejidad de la interfaz puede variar dependiendo la aplicación, por esta razón la función es sobresaliente

- Eficiencia: El usuario recibe la confirmación del envío rápidamente. Sin embargo, puede tener retrasos dependiendo la conexión de red, por esta razón la función es sobresaliente

Capturas de pantalla

- Confiabilidad: Al enviar el comando la aplicación se ejecuta en segundo plano enviando la captura silenciosamente. Ocupa una mínima cantidad de recursos y requiere conexión a la red por esta razón la función es sobresaliente

- Funcionalidad: Evidencia clara de las acciones del delincuente e información a la tuvo acceso. Lamentablemente requiere una conexión estable y constante por esta razón la función es sobresaliente

- Usabilidad: Utilizarlo es complicado ya que requiere rootear el dispositivo para poder acceder a esta funcionalidad, por esa razón la función es deficiente

- Eficiencia: Dependiendo de la aplicación el tiempo de espera para recibir la fotografía puede variar entre 5 y 10 minutos. Por esa razón la función es aceptable

Grabar pantalla

- Confiabilidad: Al ejecutar el comando la aplicación realiza lo solicitado en segundo plano. No obstante, como es un video la batería se desgasta más rápido por esta razón la función es sobresaliente

- Funcionalidad: Evidencia clara de las acciones del delincuente y toda la información a la que tiene acceso. Lamentablemente requiere una conexión estable y constante por esta razón la función es sobresaliente

- Usabilidad: Utilizarlo es complicado ya que requiere rootear el dispositivo para poder acceder a esta funcionalidad, por esa razón la función es deficiente

- Eficiencia: Dependiendo de la aplicación el tiempo de espera para recibir la fotografía puede variar entre 5 y 20 minutos. Por esa razón la función es aceptable

Tomar fotografías

- Confiabilidad: Al enviar el comando la aplicación se ejecuta en segundo plano enviando la fotografía silenciosamente. Ocupa una mínima cantidad de recursos y requiere conexión a la red por esta razón la función es sobresaliente

- Funcionalidad: Evidencia clara de las acciones del delincuente e información a la tuvo acceso. Lamentablemente requiere una conexión estable y constante por esta razón la función es sobresaliente

- Usabilidad: La función no requiere ninguna entrada y es sencilla operarla. Sin embargo, la complejidad de la interfaz puede cambiar dependiendo de la aplicación, por esta razón la función es sobresaliente

- Eficiencia: La función se ejecuta rápidamente. Sin embargo, Dependiendo de la aplicación el tiempo de espera para recibir la fotografía puede variar entre 5 y 10 minutos. Por esa razón la función es aceptable

Grabar video

- Confiabilidad: Filmar un video ocupa una cantidad considerable de batería. Sin embargo, lo hace en segundo plano por esa razón la función es aceptable

- Funcionalidad: Evidencia física del delincuente en video. Una evidencia de alto nivel, clara y sólida. Lamentablemente requiere una conexión estable y constante por esta razón la función es sobresaliente

- Usabilidad: La función requiere de algunas configuraciones y esto puede confundir al usuario. El usuario requiere de una buena conexión y un plan de datos elevado, por esta razón la función es aceptable

- Eficiencia: Dependiendo de la aplicación el tiempo de espera para recibir el video puede variar entre 5 y 20 minutos. Por esa razón la función es aceptable

Grabar audio

- Confiabilidad: Grabar el audio del dispositivo requiere de una cantidad considerable de batería. Sin embargo, lo hace en segundo plano por esa razón la función es aceptable

- Funcionalidad: Evidencia física del delincuente en video. Lamentablemente requiere una conexión estable y constante por esta razón la función es sobresaliente

- Usabilidad: La función requiere de algunas configuraciones y esto puede confundir al usuario. El usuario requiere de una buena conexión y un plan de datos elevado, por esta razón la función es aceptable

- Eficiencia: Dependiendo de la aplicación el tiempo de espera para recibir el video puede variar entre 5 y 15 minutos. Por esa razón la función es aceptable

Modo incognito

- Confiabilidad: La aplicación permanece oculta a los ojos del usuario y no existe indicios de monitoreo. El modo incognito depende de cada aplicación, por esa razón la función es sobresaliente

- Funcionalidad: El delincuente no se percata de la aplicación anti-robo y de todas sus funcionalidades. Sin embargo, un usuario experimentado puede analizar el patrón de la batería y verificar el uso de la aplicación, por esa razón la función es sobresaliente

- Usabilidad: Requiere configuración adicional y la interfaz gráfica combinado con la navegación de la aplicación es confusa, por esa razón la función es aceptable

- Eficiencia: Una vez configurada, la aplicación cambia de estado y desaparece de la interfaz gráfica del dispositivo casi al instante. No obstante, requiere configuración previa, por esa razón la función es sobresaliente

Forwarding

- Confiabilidad: La primera vez que se desvía la llamada el propietario tiene el control de la comunicación, sin embargo, el delincuente reaccionara inmediatamente impidiendo la conexión con el mismo, por esta razón la función es aceptable

- Funcionalidad: La función proporciona al usuario la posibilidad de comunicarse con el delincuente. Sin embargo, las probabilidades de que el delincuente reaccione favorablemente son mínimas, por esta razón la función es aceptable

- Usabilidad: Requiere configuración adicional y la interfaz gráfica combinada con la navegación de la aplicación es confusa, por esa razón la función es sobresaliente

- Eficiencia: El desvío de llamada puede malgastar el tiempo del usuario, ya que el delincuente puede cerrar la llamada, por esa razón la función es aceptable

Activar/desactivas funciones

- Confiabilidad: El delincuente puede percatarse de los cambios realizados en el dispositivo si lo está utilizando sincrónicamente con el usuario, por esa razón la función es aceptable

- Funcionalidad: Si se utiliza estratégicamente, activar y/o desactivar funciones puede facilitar el rastreo, así como impedir el uso de información restringida por parte del delincuente, por esa razón la función es sobresaliente

- Usabilidad: La interfaz gráfica de las aplicaciones es muy intuitiva al desactivas o activar funciones. Está diseñado para que el usuario actúe rápido durante la emergencia, por esa razón la función es sobresaliente

- Eficiencia: Está diseñado para que el usuario actúe rápido durante la emergencia. Sin embargo, por esa razón la función es sobresaliente

Terminal de android

- Confiabilidad: La terminal de Android es una terminal Linux que permite ejecutar varios comandos. Sin embargo, el delincuente puede percatarse fácilmente de las acciones remotas del usuario, por esa razón la función es aceptable

- Funcionalidad: La terminal es una herramienta muy poderosa y precisa ya que ejecuta múltiples funciones en poco tiempo, por esa razón la función es sobresaliente

- Usabilidad: Lamentablemente solo usuarios avanzados pueden generar una estrategia que beneficie el rastreo del dispositivo, por esa razón la función es deficiente

- Eficiencia: La herramienta es muy versátil y brinda funciones únicas para recuperar el dispositivo. Sin embargo, el uso de la herramienta requiere experticia, por esa razón la función es aceptable

Información del dispositivo

- Confiabilidad: La información está disponible siempre que la conexión a la red se estable, por esa razón la función es sobresaliente

- Funcionalidad: Dependiendo de la aplicación la información disponible puede variar, en su mayoría brinda información necesaria, por esa razón la función es sobresaliente

- Usabilidad: La interfaz y el flujo de navegación de la aplicación es sencilla. Sin embargo, la información proporcionada puede confundir a usuarios inexpertos, por esa razón la función es sobresaliente

- Eficiencia: La información llega al usuario casi al instante, puede variar dependiendo el estado de la red, por esa razón la función es sobresaliente

Modo de emergencia

- Confiabilidad: Se ejecutan varias acciones que alertaran al delincuente. Es posible que corte la comunicación de la red o apague el dispositivo. Si el modo emergencia es discreto las posibilidades de éxito incrementan, por esa razón la función es insuficiente

- Funcionalidad: Si el modo emergencia es discreto, el usuario obtiene una ventaja sobre el delincuente ya que ejecuta varias acciones al mismo tiempo y constantemente. Sin embargo, la conexión es un factor importante, por esa razón la función es aceptable

- Usabilidad: El modo emergencia se ejecuta rápidamente si el usuario lo activa, es el componente más importante de la interfaz, por esa razón la función es sobresaliente

- Eficiencia: La función no requiere un tiempo considerable para n ejecutarse. No obstante, el beneficio del usuario depende de la conexión y de la confiabilidad del mismo, por esa razón la función es aceptable

Fakeshutdown

- Confiabilidad: La interfaz gráfica que genera la función proporciona un diseño estándar y por lo tanto poco personalizado para el dispositivo, por esa razón la función es insuficiente

- Funcionalidad: Un usuario avanzado puede percatarse de la interfaz de apagado y desactivar la comunicación con el dispositivo, de igual manera puede apagar el dispositivo mediante un hardreset, por esa razón la función es insuficiente

- Usabilidad: La interfaz y el flujo de navegación son aceptables para el usuario, por esa razón la función es sobresaliente

- Eficiencia: El usuario no malgasta tiempo activando la función, sin embargo, si el delincuente se percata de la existencia de una aplicación anti-robo el beneficio es nulo, por esa razón la función es insuficiente

Iniciar aplicaciones/servicios

- Confiabilidad: Permite iniciar varios servicios y aplicaciones remotamente. Sin embargo, el delincuente puede percatarse fácilmente de las acciones remotas del usuario, por esa razón la función es aceptable

- Funcionalidad: Es una herramienta muy poderosa y precisa ya que ejecuta múltiples funciones en poco tiempo, por esa razón la función es sobresaliente

- Usabilidad: Lamentablemente solo usuarios avanzados pueden generar una estrategia que beneficie el rastreo del dispositivo, por esa razón la función es deficiente

- Eficiencia: La herramienta es muy versátil y brinda funciones únicas para iniciar servicios y aplicaciones. Sin embargo, el uso de la herramienta requiere experticia, por esa razón la función es aceptable

Copias de seguridad

- Confiabilidad: La copia de seguridad se realiza silenciosamente y dependiendo de la aplicación se realiza una copia de todo el dispositivo. El delincuente no puede darse cuenta ya que se ejecuta en segundo plano y no consumo muchos recursos, por esa razón la función es sobresaliente

- Funcionalidad: Garantiza la disponibilidad de los datos a pesar de que el dispositivo está desaparecido, siempre que exista una comunicación a la red estable, por esa razón la función es sobresaliente

- Usabilidad: Requiere configuración adicional y la interfaz gráfica combinado con la navegación de la aplicación es confusa, por esa razón la función es aceptable

- Eficiencia: La velocidad en las aplicaciones recuperan los datos depende de la red. Sin embargo, la cantidad de información de un dispositivo inteligente es cuantiosa y el tiempo de trasferencia de datos demora, por esa razón la función es aceptable

Tabla 9: Resultado análisis de métricas

	Confiabilidad	Funcionalidad	Usabilidad	Eficiencia
Alarma	4	2	4	4
Borrado	4	3	2	2
Bloqueo	3	4	4	4
Geolocalización	4	2	4	4
Mensajes	4	2	4	4
Capturas de pantalla	4	4	1	3

Grabar Pantalla	3	4	1	3
Tomar Fotografías	4	4	3	3
Grabar Videos	3	4	3	3
Grabar Audio	3	4	3	3
Modo Incognito	4	4	2	4
Forwarding	3	3	3	3
Activar/desactivar funciones	3	4	2	3
Terminal de Android	3	4	1	3
Información Dispositivo	4	4	4	4
Modo Emergencia	3	4	4	4
FakeShutdown	2	4	4	2
Iniciar aplicaciones/servicios	3	4	1	3
Copias de seguridad	4	4	3	3

Mejora de funcionalidades

Se propone una mejora en las funcionalidades mediante varios factores, estos son:

- Propuesta de valor: Valor agregado que se le quiere dar a la función
- Factibilidad: Es una consideración técnica y se requiere analizar profundamente si los cambios propuestos pueden realizarse
- Deseabilidad: Es la experiencia del usuario centrada en la parte del análisis. Toma en consideración las necesidades del usuario final, la interacción de los elementos, posibilidades y como se van a comercializar o vender
- Viabilidad: Finalmente, la viabilidad del trabajo debe considerarse como una función del negocio en general. La viabilidad también incluye factores relacionados con la industria, el entorno regulatorio y la supervisión financiera, o consideraciones legales.

Alarma

- Propuesta de valor: Reproducir sonido personalizado de texto a voz
- Factibilidad: La implementación puede desarrollarse mediante la API de Android Studio Text to Speech
- Deseabilidad: Interfaz sencilla en la cual se pueda enviar el comando a través de mensajes SMS o por interfaz web
- Viabilidad: No existe ninguna consideración legal importante y el costo de la implementación es factible

Bloqueo

- Propuesta de valor: Bloquear hardware específico
- Factibilidad: Se puede implementar funciones con eventos que permitan el bloqueo de botones
- Deseabilidad: Impedir que el usuario controle el dispositivo o ejecute aplicaciones que bloquen el mismo
- Viabilidad: No existe ninguna consideración legal importante y el costo de la implementación es factible

Geolocalización

- Propuesta de valor: Ubicación sin conexión
- Factibilidad: Guardar variables latitud y longitud en la base de datos local del dispositivo
- Deseabilidad: Guardar coordenadas y enviarlas cuando existe una conexión estable con el administrador web
- Viabilidad: No existe ninguna consideración legal importante y el costo de la implementación es factible

Captura de pantalla

- Propuesta de valor: Cronograma de capturas
- Factibilidad: Utilizando la API de AlarmManager, esto permite programar aplicación para que se ejecuté en algún momento en el futuro
- Deseabilidad: Organizar horarios estratégicos a través de una interfaz sencilla
- Viabilidad: Costo de implementación alto

Grabar pantalla

- Propuesta de valor: Grabar audio y video externo al mismo tiempo
- Factibilidad: Utilizando MediaMixer de Android Studio API la aplicación puede grabar múltiples canales al mismo tiempo
- Deseabilidad: Permite conocer el entorno del delincuente mientras captura audio y video del dispositivo
- Viabilidad: Costo de implementación bajo. Sin embargo, en la integración pueden presentarse dificultades

Tomar fotografías

- Propuesta de valor: Disparadores personalizados
- Factibilidad: Utilizando la Camera API de Android Studio se pueden establecer parámetros dinámicos para que el usuario ingrese sus propios disparadores
- Deseabilidad: El usuario configura un disparador cuando el delincuente ejecute o realice alguna acción configurada por el usuario se toma una fotografía
- Viabilidad: Costo de implementación medio

Grabar videos y audio

- Propuesta de valor: Visualizar video o audio en vivo
- Factibilidad: Utilizando el FrameworkVitamio SDK
- Deseabilidad: El usuario puede visualizar o escuchar el entorno del dispositivo en tiempo real
- Viabilidad: No existe ninguna consideración legal importante y el costo de la implementación es factible

Activar / Desactivar funciones, servicios y terminal

- Propuesta de valor: Establecer disparadores modelo
- Factibilidad: Utilizando la API TriggerEventListener se puede desarrollar disparadores que se activen cuando el usuario interactúe con la interfaz
- Deseabilidad: Disminuye tiempo de reacción al recuperar el dispositivo
- Viabilidad: No existe ninguna consideración legal importante y el costo de la implementación es factible

Modo emergencia

- Propuesta de valor: Ejecutar acciones personalizadas
- Factibilidad: Utilizando la API TriggerEventListener se puede desarrollar disparadores que se activen cuando el usuario interactúe con la interfaz
- Deseabilidad: Establecer modelos que permitan al usuario ejecutar varios comandos y priorizar ejecución
- Viabilidad: No existe ninguna consideración legal importante y el costo de la implementación es factible

Fakeshutdown

- Propuesta de valor: Personalizar botón dependiendo el dispositivo
- Factibilidad: Trabajar en programación front-end

- Deseabilidad: El diseño del botón implica la credibilidad de la función. Personalizando el diseño para cada dispositivo la función tiene una alta probabilidad de éxito
- Viabilidad: No existe ninguna consideración legal importante y el costo de la implementación es factible

5. Conclusiones y Recomendaciones

5.1 Conclusiones

- La principal desventaja encontrada fue que las aplicaciones anti-robo no pueden reaccionar ante un fallo de comunicación de las redes móviles

- La principal ventaja encontrada fue que las aplicaciones anti-robo comprenden una capa de seguridad muy pragmática y fácil de utilizar en los dispositivos móviles. Existen múltiples funcionalidades que permiten recuperar nuestro dispositivo utilizando el hardware y software del sistema operativo Android

- Entre los mecanismos anti-robo más importantes, se incluye bloquear el dispositivo remotamente, eliminar la información del dispositivo remotamente, geolocalizar remotamente mediante APIs (la más común Google Maps), enviar mensajes SMS y MMS, autenticación de usuarios, logs, deshabilitar sincronización de datos y bloquear dispositivo por número de intentos

- Las aplicaciones antirrobo poco prácticas en ambientes donde el delincuente desactiva las funcionalidades de red y elimina la aplicación rápidamente

- De las cinco aplicaciones distintas que se compararon, se enfoca en funcionalidades primordiales, bloqueo, borrado y geolocalización

- La mayoría de las funcionalidades anti-robo se aplican durante y después de la pérdida del dispositivo

- La confiabilidad, funcionalidad, usabilidad y eficiencia de las funciones anti-robo cumplen en su mayoría con un alto puntaje de evaluación

- Encontrar mi dispositivo se enfoca a funcionalidades primordiales, bloqueo, borrado y geolocalización

- La principal desventaja de Encontrar mi dispositivo es no incluir funciones extra que el usuario podría utilizar para identificar al delincuente, además es poco práctica en ambientes donde el delincuente desactiva las funcionalidades de red y elimina la aplicación rápidamente

- La principal ventaja de Encontrar mi dispositivo son los servicios de Google para analizar el historial de todas las ubicaciones del dispositivo. Su principal desventaja es la limitación de funcionalidades

- Cerberus anti-theft tiene múltiples funcionalidades, y comparativamente es el que más funcionalidades brinda

- La principal ventaja de Cerberus anti-theft son sus múltiples funcionalidades que permiten al propietario manipular el escenario y hasta engañar al delincuente que no existe control por parte de Cerberus

- La principal desventaja de Cerberus anti-theft es la limitación entre la comunicación del dispositivo y los comandos enviados a través de SMS o internet (JSON)

- Prey anti-theft está consolidado como una de las mejores aplicaciones anti-robo, la mayoría de sus funcionalidades son gratuitas y son efectivas en escenarios reales

- La principal ventaja de Prey anti-theftes que sus funcionalidades son gratuitas, además que su interfaz es muy intuitiva para el usuario

- La principal desventaja de Prey anti-theft es la limitación de funcionalidades extra como capturas de pantalla, grabar videos y audios, activar/desactivar funcionalidades del dispositivo móvil, etc. Y ciertas funcionalidades requieren rootear el dispositivo

- Avast Anti-theft invita al usuario inexperimentado a probar un nuevo tipo de seguridad, es una marca con confianza y sus funcionalidades proporcionan comodidad y ejecución rápida, lamentablemente Avast requiere un pago mensual

- La principal ventaja de Avast Anti-theft es la ejecución de sus funcionalidades. No requieren mucho tiempo de respuesta y son muy pragmáticas en situaciones de emergencia

- La principal desventaja de Avast Anti-theft son sus funcionalidades extras. No existe un diferenciador importante con otras aplicaciones como Cerberus y Prey

- Wheres my Droid es una aplicación desactualizada, sin embargo, sus funcionalidades logran cumplir el objetivo de recuperar el dispositivo, no obstante, en comparativa con las otras aplicaciones tiene limitación de funcionalidades

- La principal ventaja de Where's my Droid es la ejecución de funcionalidades principales como rastrear el dispositivo, eliminar información, bloquear y tomar fotografías

- Cerberus Anti-Theft es la aplicación privada más recomendada y Prey anti-theft es la aplicación Open Source más recomendada

5.2 Recomendaciones

- Se recomienda utilizar las funciones con mayor efectividad en las aplicaciones anti-robo. Estas son bloqueo, borrado, copias de seguridad, fotografías, capturas de pantalla y modo incógnito

- Se recomienda al usuario activar el modo incógnito desde el momento de instalación de la aplicación

- Se sugiere utilizar la aplicación Prey anti -theft si el usuario prefiere una alternativa open source y utilizar la aplicación Cerberus anti-theft si el usuario prefiere pagar por la aplicación

- Se sugiere estudiar las funciones en la página web oficial de cada aplicación para entender y utilizar todo el potencial y beneficios que proporciona una protección anti-robo

- Se recomienda activar los datos móviles automáticamente si el wi-fi deja de funcionar, esto para que la aplicación anti-robo pueda responder rápidamente en un escenario de emergencia

- Se sugiere rootear el dispositivo para poder autorizar y así utilizar todas las funcionalidades de aplicaciones anti-robo como el grabar la pantalla del dispositivo

- Se recomienda enviar los comandos a través de SMS, siempre que se pierda la conexión de una red Wi-Fi o datos móviles

- Se sugiere profundizar la investigación con herramientas de análisis forense en la aplicación open source Prey Anti theft para validar nuevos resultados

- Para el desarrollo de nuevas funcionalidades anti-robo se recomienda entender el funcionamiento de las APIs de Android en conjunto con su hardware

- Se recomienda actualizar el dispositivo Android y su aplicación anti-robo a la última versión de producción

- Se sugiere utilizar una aplicación antirrobo por dispositivo y no instalar varias aplicaciones anti-robo que generen conflicto entre funciones

- Se recomienda configurar un número de teléfono alternativo para gestionar comandos SMS

6. Bibliografía

Engebretson, P. (2013). *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier. p.129

Simon, L., & Anderson, R. (2015). Security Analysis of Consumer-Grade Anti-Theft Solutions Provided by Android Mobile Anti-Virus Apps (p. 11). Cambridge. Retrieved from https://www.cl.cam.ac.uk/~rja14/Papers/mav_most15.pdf

Cerberus Anti Theft - Official Website(P., 2013). *Cerberusapp.com*. N.p., 2017. Web. 15 Mayo 2017. (P., 2013)

Prey: Open source theft recovery [LWN.net]. (2011). Lwn.net. Recuperado 22 Mayo 2017, desde https://lwn.net/Articles/450221/

Overview: What is Prey and how it can help you - Prey Knowledge Base. (2016). Help.preyproject.com. Recuperado 22 Mayo 2017, de http://help.preyproject.com/article/185-overview-what-is-prey

SANS Institute. (2012). Analyzing Network Traffic With Basic Linux Tools (p. 19). Maryland. Recuperado desde https://www.sans.org/reading-room/whitepapers/protocols/analyzing-network-traffic-basic-linux-tools-34037

Abdul Qader, M., Shan Khan, A., &Naved Qureshi, M. (2014). Anti-Theft Application for Android Based Devices. Recuperado de https://www.researchgate.net/publication/271482528_Anti-theft_application_for_android_based_devices

Analyze Your Build with APK Analyzer | Android Studio. (2017). Developer.android.com. Recuperado el 28 May 2017, de https://developer.android.com/studio/build/apk-analyzer.html

Funcionalidades antirobo | Prey. (2017). Preyproject.com. Recuperado 12 June 2017, de https://www.preyproject.com/es/caracteristicas

Austin, J., Leong, F., & Frederick Leong. (2006). The Psychology Research Handbook: A Guide for Graduate Students and Research Assistants (Second Edition) (1st ed.). Sage Publications.

Privacy in the Age of the Smartphone | Privacy Rights Clearinghouse. (2017). Privacyrights.org. Recuperado 23 June 2017, de https://www.privacyrights.org/consumer-guides/privacy-age-smartphone

The Washington Post. (2017). WikiLeaks: The CIA is using popular TVs, smartphones and cars to spy on their owners. Recuperado de https://www.washingtonpost.com/news/the-switch/wp/2017/03/07/why-the-cia-is-using-your-tvs-smartphones-and-cars-for-spying/?utm_term=.2ef1b7d567e2

Abirami, D., Anantha, S., Annapoorani, S., & Padma, M. (2014). An Intelligent Anti-Theft Android application.

The Journal of Digital Forensic Security and Law. (2014). EFFECTS OF THE FACTORY RESET ON MOBILE DEVICES (p. 16). Association of Digital Forensics, Security and Law. Recuperado de http://ojs.jdfsl.org/index.php/jdfsl/article/view/280/225

Ministerio Coordinador de Seguridad. *Robo A Celulares Encabeza Lista De Artículos Sustraídos*. 2014. Web. 15 Mayo 2017.

Asociación GSM. *La Economía Móvil América Latina 2016*. 2016. Web. 15 Mayo 2017.

Curso de seguridad en dispositivos móviles. (2017). Bratislava.

Lynda,com. (2016). Static analysis of applications. Recuperado de https://www.lynda.com/Android-tutorials/Static-analysis-applications/512725/565236-4.html#tab

Lynda.com. (2016). Dynamic analysis of applications. Recuperado de https://www.lynda.com/Android-tutorials/Dynamic-analysis-applications/512725/565237-4.html

Taj El-Dean Osman, N., Mohammed Al-Noor, S., & Mohammed Ali, T. (2017). Tracking stolen android phone system (p. 78). Recuperado de http://repository.sustech.edu/bitstream/handle/123456789/12813/Tracking%20stolen%20phones.pdf?sequence=1

GPS based vehicle and person tracking system. (2017). gpstracking. Recuperado el 18 August 2017, de http://www.gpstracking.co.in/documents/Introduction%20To%20GPS%20Vehicle%20or%20Person

Back Up Data. (2013). Baylor University. Recuperado 18 August 2017, de http://www.baylor.edu/content/services/document.php/192120.pdf

Data Backup and Restore using Windows 7 (p. 18). Recuperado de https://www.ucc.ie/en/media/support/computercentre/trainingmanuals/BackUpandRestore.pdf

Kulkarni, B. (2012). ANTI THEFT SYSTEMS | EngineersGarage. Engineersgarage.com. Recuperado el 29 Agosto 2017, from https://www.engineersgarage.com/articles/anti-theft-systems

Defcon 21. (2013). Defcon 21 - The Secret Life of SIM Cards. Recuperado desde https://www.youtube.com/watch?v=31D94QOo2gY

Wipe Data. (2017). Disk-partition.com. Recuperado el 29 August 2017, from http://www.disk-partition.com/help/wipe-data.html

Dictionary, a. (2017). anti-theft Meaning in the Cambridge English Dictionary. Dictionary.cambridge.org. Recuperado el 1 September 2017, from http://dictionary.cambridge.org/dictionary/english/anti-theft

Find, lock, or erase a lost Android device - Google Account Help. (2017). Support.google.com. Retrieved 1 September 2017, from https://support.google.com/accounts/answer/6160491?hl=en

Shedge, K., Dhatrak, D., &Ugale, K. (2017). Mobile Theft Tracking Application. pdf.

Enriquez, J., & Casas, S. (2013). Usabilidad en aplicaciones móviles. Río Gallego.

Nayebi, F., Desharnais, J., &Abran, A. (2017). The State of the Art of Mobile Application Usability Evaluation. Pdf, Quebec.

Granollers, T., &Lóres, J. (2004). Esfuerzo de Usabilidad: un nuevo concepto para medir la usabilidad de un sistema interactivo basada en el Diseño Centrado en el Usuario. Lleida.

Alluri, A. (2012). USABILITY TESTING OF ANDROID APPLICATIONS (p. 60). San Diego. Recuperado desde https://sdsudspace.calstate.edu/bitstream/handle/10211.10/3556/Alluri_Aruna.pdf?sequence=1

Android Testing Cheat Sheet - OWASP. (2017). Owasp.org. Recuperado el 8 September 2017, from https://www.owasp.org/index.php/Android_Testing_Cheat_Sheet

Lee, P. (2016). Privacy of Network Traffic in Anti-Theft Software (p. 8). Massachusetts. Recuperado desde http://www.cs.tufts.edu/comp/116/archive/fall2016/plee.pdf

Prey. (2017). GitHub. Recuperado el 26 September 2017, from https://github.com/prey

Gagnon, F., Ferland, M., Fortier, M., Desloges, S., Ouellet, J., & Boileau, C. (2015). AndroSSL: A Platform to Test Android Applications Connection Security (p. 8). Canada. Retrieved from http://www2.cegep-ste-foy.qc.ca/freesite/fileadmin/users/501/publications/GagnonF_AndroSSL_FPS15_Paper.pdf

Trummer, T., & Dalvi, T. (2015). Mobile SSL Failures (p. 7). Londres. Recuperado de https://www.blackhat.com/docs/ldn-15/materials/london-15-Trummer-Dalvi-The-Savage-Curtain-Mobile-SSL-Failures-wp.pdf

IBM Knowledge Center. (2017). Ibm.com. Recuperado el 26 de Octubre 2017, desde https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.html

Training, G. (2017). 1.0: Introduction to Android · Android Developer Fundamentals Course – Concepts. Google-developer-training.gitbooks.io. Retrieved 27 October 2017, from https://google-developer-training.gitbooks.io/android-developer-fundamentals-course-concepts/content/en/Unit%201/10_c_intro_to_android.html

Jensen, C. (2015). APIs For Dummies, IBM Limited Edition (p. 57). Nueva York: John Wiley & Sons, Inc.

Kuma, R., Pawar, L., & Aggarwal, A. (2014). Smartphone's Hardware Architectures and Their Issues (p. 3). Mohali: Chandigarh University. Retrieved from https://www.academia.edu/7676259/Smartphones_Hardware_Architectures_and_Their_Issues?auto=download

Al-Aubidy, K. RISC Architecture. PDF, Aman.

Chuang, Y. (2010). ARM Architecture. Pdf, Taipéi.

About the iOS Technologies. (2017). Developer.apple.com. Retrieved 13 November 2017, from https://developer.apple.com/library/content/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/Introduction/Introduction.html

About - Google Maps. (2017). Google.com. Retrieved 16 November 2017, from https://www.google.com/maps/about/

Geolocation with Google Maps. Static.googleusercontent.com. Retrieved 16 November 2017, from https://static.googleusercontent.com/media/enterprise.google.com/es//maps/files/geolocation_leaflet.pdf

Ratsameethammawong, P., &Kasemsan, M. (2010). Mobile Phone Location Tracking by the Combination of GPS, Wi-Fi and Cell Location Technology (p. 7). Bangkok. Retrieved from http://ibimapublishing.com/articles/CIBIMA/2010/566928/566928.pdf

Shan Khan, A., Qureshi, M., & Qadeer, M. (2014). Anti-theft application for android based devices (p. 5). Nueva Delhi. Retrieved from https://www.researchgate.net/publication/271482528_Anti-theft_application_for_android_based_devices

Varma, V. (2012). Wireless Fidelity—WiFi (p. 2). Retrieved from https://www.ieee.org/about/technologies/emerging/wifi.pdf

Henniges, R. (2012). Current approches of Wifi Positioning (p. 8). Berlin. Retrieved from https://www.snet.tu-berlin.de/fileadmin/fg220/courses/WS1112/snet-project/wifi-positioning_henniges.pdf

Estes, B. (2016). Geolocation—The Risk and Benefits of a Trending Technology. Isaca.org. Retrieved 23 November 2017, from https://www.isaca.org/Journal/archives/2016/volume-5/Pages/geolocation-the-risk-and-benefits-of-a-trending-technology.aspx

LTE: The Future of Mobile Broadband Technology. (2009) (p. 19). Nueva Jersey. Retrieved from http://innovation.verizon.com/content/dam/vic/PDF/LTE%20The%20Future%20of%20Mobile%20Broadband%20Technology.pdf

GSM - About Us. (2017). About Us. Retrieved 28 November 2017, from https://www.gsma.com/aboutus/gsm-technology/gsm

Ibm.com. (2018). IBM Knowledge Center. [online] Available at: https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.14/gtps7/s7symm.html [Accessed 21 Jan. 2018].

Msdn.microsoft.com. (2018). Asymmetric Keys (Windows). [online] Available at: https://msdn.microsoft.com/es-es/library/windows/desktop/aa387460(v=vs.85).aspx [Accessed 21 Jan. 2018].

Google Maps Geolocation API | Google Maps Geolocation API | Google Developers. (2018). Google Developers. Retrieved 26 January 2018, from https://developers.google.com/maps/documentation/geolocation/intro?hl=es-419

Introducción a la Google Maps Android API | Google Maps Android API | Google Developers. (2018). Google Developers. Retrieved 26 January 2018, from https://developers.google.com/maps/documentation/android-api/intro?hl=es-419

Bing Maps REST Services. (2018). Msdn.microsoft.com. Retrieved 26 January 2018, from https://msdn.microsoft.com/en-us/library/ff701713.aspx

OpenLayers - Welcome. (2018). Openlayers.org. Retrieved 26 January 2018, from http://openlayers.org

About Wi-Fi positioning - Combain. (2018). Combain. Retrieved 27 January 2018, from https://combain.com/about/about-positioning/wi-fi-positioning/

Zahradnik, F. (2017). How a Wi-Fi Positioning System Works to Determine Your Location. Lifewire. Retrieved 28 January 2018, from https://www.lifewire.com/wifi-positioning-system-1683343

ArchundiaPapacetzi, F. (2003). Wireless Personal Area Network (WPAN) & Home Networking (p. 80). México. Retrieved from http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/archundia_p_fm/capitulo3.pdf

Singh, P., Kumar Sharma, D., & Agrawal, S. (2011). A Modern Study of Bluetooth Wireless Technology (p. 9). Chhattisgarh. Retrieved from https://pdfs.semanticscholar.org/d5cc/64bd33521f2bcd018576061ce5642dc17963.pdf

Tan, G., Miu, A., Guttag, J., & Balakrishnan, H. (2001). Forming Scatternets from Bluetooth Personal Area Networks (p. 11). Massachusetts: The NMS group at MIT's Computer Science and Artificial Intelligence Laboratory. Retrieved from http://nms.csail.mit.edu/projects/Blueware/tr826.pdf

MediaRecorder | Android Developers. (2018). Developer.android.com. Retrieved 5 February 2018, from https://developer.android.com/guide/topics/media/mediarecorder.html

Yu, X., Wang, Z., Sun, K., Tao Zhu, W., Gao, N., & Jing, J. (2014). Remotely Wiping Sensitive Data on Stolen Smartphones (p. 6). Virginia. Retrieved from http://csis.gmu.edu/ksun/publications/wipeout-asiaccs2014.pdf

Focus on property crime: year ending March 2016. (2016) (p. 41). london. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/focusonpropertycrime/yearendingmarch2016#mobile-phone-theft

A Technology Brief on SSL/TLS Traffic. (2016) (p. 10). Mountain View. Retrieved from https://www.symantec.com/content/dam/symantec/docs/data-sheets/technology-brief-ssl-tls-traffic-en.pdf

Seguridad con HTTPS y SSL. (2018) (p. 1). Retrieved from https://developer.android.com/training/articles/security-ssl.html?hl=es-419

lsaleh, M., Alomar, N., &Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. PLOS ONE, 12(3), e0173284. http://dx.doi.org/10.1371/journal.pone.0173284

Raymond, V., &Sushmitha, E. (2017). Google drive based secured anti-theft android application. 2017 International Conference OnIot And Application (ICIOT). http://dx.doi.org/10.1109/iciota.2017.8073623

Akiyama, T., Teranishi, Y., Okamura, S., &Shimojo, S. (2009). A Consideration of the Precision Improvement in WiFi Positioning System. 2009 International Conference On Complex, Intelligent And Software Intensive Systems. http://dx.doi.org/10.1109/cisis.2009.148

Chang, S., Lu, T., & Song, H. (2016). SmartDog: Real-Time Detection of Smartphone Theft. 2016 IEEE International Conference On Internet Of Things (Ithings) And IEEE Green Computing And Communications (Greencom) And IEEE Cyber, Physical And Social Computing (Cpscom) And

IEEE Smart Data (Smartdata). http://dx.doi.org/10.1109/ithings-greencom-cpscom-smartdata.2016.61

Overview, S. (2018). Sensors Overview | Android Developers. Developer.android.com. Retrieved 16 February 2018, from https://developer.android.com/guide/topics/sensors/sensors_overview.html

Apple Inc. (2017). Finger biometric sensor including drive signal level updating and related methods. Cupertino.

Roy, S., Shah, A., & Bhattacharya, U. (2016). Touch and Track: An Anti-theft and Data Protection Technique for Smartphones. Communications In Computer And Information Science, 347-357. http://dx.doi.org/10.1007/978-981-10-2738-3_30

Device anti-theft. (2018). T-Mobile Support. Retrieved 22 February 2018, from https://support.t-mobile.com/docs/DOC-21135

Tarjeta SIM: que son y como funcionan en nuestros smartphones. (2018). Androi2id. Retrieved 22 February 2018, from https://andro2id.com/tarjeta-sim-funcionan-smartphones/

Esteban, N. REDES CELULARES (GSM, GPRS) (p. 27). Rosario: UNIVERSIDAD NACIONAL DE ROSARIO. Retrieved from https://www.dsi.fceia.unr.edu.ar/downloads/distribuidos/material/monografias/RedesGSM.pdf

ARCHANA, R., BHUVANESHWARI, E., & HEMAVATHI, T. (2015). MULTIMEDIA MESSAGING SERVICE (MMS) BASED ANTITHEFT APPLICATION. International Journal Of Innovative Trends And Emerging Technologies, 1(Special Issue 2(ICITET 15), 5.

C, L., P, A., & S, S. (2009). Biometric Anti-theft and Tracking System for mobiles - BATS. International Journal Of Recent Trends In Engineering, Vol 1(No. 1), 6.

Dospinescu, O., &Lîsîi, I. (2016). The Recognition of Fingerprints on Mobile Applications — an Android Case Study. Journal Of Eastern Europe Research In Business And Economics, 1-11. http://dx.doi.org/10.5171/2016.813264

Kuriakose, P., & K, A. (2017). Secured Android Application Using Biometric Authentication. International Journal Of Innovative Research In Computer And Communication Engineering, 5(4), 5.

Markovski, S., Kuzmanovska, A., &Simeonovski, M. (2012). A Protocol for Secure SMS Communication for Android OS. Advances In Intelligent And Soft Computing, 171-178. http://dx.doi.org/10.1007/978-3-642-28664-3_15

Arquitectura de la plataforma | Android Developers. (2018). Developer.android.com. Retrieved 23 February 2018, from https://developer.android.com/guide/platform/index.html?hl=es-419

Shaheen, J., Asghar, M., & Huss, A. (2017). Android OS with its Architecture and Android Application with Dalvik Virtual Machine Review. International Journal Of Multimedia And Ubiquitous Engineering, 12(7), 12.

Mohmedhussen, A., &Altaee, W. (2017). Comparison of Android and iPhone Operating System. International Journal Of Computer Applications, 167(2), 6.

Schmidt, D. (2017). Infrastructure Middleware (Part 1): Hardware Abstraction Layer (HAL) (p. 33). Nashville. Retrieved from http://www.dre.vanderbilt.edu/~schmidt/cs891f/2017-PDFs/L4-pt1-HAL.pdf

Linares-Vasquez, M., Bavota, G., & Escobar-Velasquez, C. (2017). An Empirical Study on Android-Related Vulnerabilities. 2017 IEEE/ACM 14Th International Conference On Mining Software Repositories (MSR). http://dx.doi.org/10.1109/msr.2017.60

Umasankar. (2017). Analysis of latest vulnerabilities in android. 2017 International Conference On Advances In Computing, Communications And Informatics (ICACCI). http://dx.doi.org/10.1109/icacci.2017.8126011

Jimenez, M., Papadakis, M., Bissyande, T., & Klein, J. (2016). Profiling Android Vulnerabilities. 2016 IEEE International Conference On Software Quality, Reliability And Security (QRS). http://dx.doi.org/10.1109/qrs.2016.34

NEW TRACKING ROOTKIT AT APPLICATION LAYER IN ANDROID. (2017). International Journal Of Advance Engineering And Research Development, 4(04). http://dx.doi.org/10.21090/ijaerd.co007

ARM Architecture Reference Manual. (2005) (p. 1138). Cambridge. Retrieved from https://www.scss.tcd.ie/~waldroj/3d1/arm_arm.pdf

ARM Information Center. (2018). Infocenter.arm.com. Retrieved 1 March 2018, from http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.ddi0210c/Cihhcjia.html

Canel, S. (2007). Microcontroladores ARM Advanced RISC Machine (p. 35). Buenos Aires. Retrieved from http://www.electron.frba.utn.edu.ar/upload/Materias/95-0429/archivos/Cap10_2009_ARM7_apunte.pdf

Chuang, Y. (2010). ARM Architecture (p. 26). Taiwan. Retrieved from https://www.csie.ntu.edu.tw/~cyy/courses/assembly/10fall/lectures/handouts/lec08_ARMarch.pdf

ARM Architecture Overview. Web.eecs.umich.edu. Retrieved 1 March 2018, from https://web.eecs.umich.edu/~prabal/teaching/eecs373-f10/readings/ARM_Architecture_Overview.pdf

Administración de ABI | Android Developers. (2018). Developer.android.com. Retrieved 1 March 2018, from https://developer.android.com/ndk/guides/abis.html?hl=es-419

Chowdhury, S., &Ghosal, P. (2015). Enterprise Application Security in Android Devices Using Short Messaging Service under Unified Communication Framework. 2015 IEEE 12Th Intl Conf On Ubiquitous Intelligence And Computing And 2015 IEEE 12Th Intl Conf On Autonomic And Trusted Computing And 2015 IEEE 15Th Intl Conf On Scalable Computing And Communications And Its Associated Workshops (UIC-ATC-Scalcom). http://dx.doi.org/10.1109/uic-atc-scalcom-cbdcom-iop.2015.140

SHRIWAS, M., GUPTA, N., & SINHA, A. (2013). BACKUP AND RESTORE DATA IN ANDROID. INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY, 1(8). Retrieved from https://www.researchgate.net/publication/304313463_BACKUP_AND_RESTORE_DATA_IN_ANDROID

MediaRecorder | Android Developers. Retrieved from https://developer.android.com/reference/android/media/MediaRecorder.html

Shedge, P., Dhatrak, D., &Ugale, K. (2017). Mobile Theft Tracking Application. International Research Journal Of Engineering And Technology (IRJET), 4(1), 4. Retrieved from https://www.irjet.net/archives/V4/i1/IRJET-V4I1105.pdf

7. Anexo

7.1. Glosario de términos

7.2. A

7.2.1.Android

Sistema operativo basado en el núcleo de Linux

7.2.2.Advanced RISC Architecture

Es una arquitectura RISC (Ordenador con Conjunto Reducido de Instrucciones) de 32bits

7.2.3.Ataque de canal lateral

Es un ataque basado en información obtenida gracias a la propia implementación física de un sistema informático

---

7.3. B

7.3.1.Bluetooth

Es unaespecificación industrial para Redes Inalámbricas de Área Personal (WPAN)

7.3.2.Búfer de Datos

Es un espacio de memoria, en el que se almacenan datos de manera temporal

---

7.4. E

7.4.1.Entorno de desarrollo integrado

Es una aplicación informática que proporciona servicios integrales para facilitarle al programador el desarrollo de software

---

7.5. F

7.5.1. Framework

Es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar

7.5.2. Freemium

Es un modelo de negocio que funciona ofreciendo servicios básicos gratuitos, mientras se cobra por otros más avanzados o especiales

7.5.3. Forwarding

Es la acción de redirigir un puerto de red de un nodo de red a otro

---

7.6. I

7.6.1. Interfaz de programación de aplicaciones

Es un conjunto de subrutinas, funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción

7.6.2. IP

Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo

---

7.7. J

7.7.1. Javascript

Es un lenguaje de programación interpretado orientado a objetos

---

7.8. K

7.8.1. Kit de desarrollo de software

Conjunto de herramientas de desarrollo de software que le permite al programador crear una aplicación informática para un sistema concreto

---

7.9. M

7.9.1.Marketplace

Son plataformas online creadas por una empresa que actúa como un tercero neutral para poner en contacto a compradores y vendedores

7.9.2.Memoria Cache

Es un tipo de memoria volátil. Su función es almacenar instrucciones y datos a los que el procesador debe acceder continuamente

7.9.3.Media Access Control

Es un identificador de 48 bits (6 bloques de dos caracteres hexadecimales (4 bits)) que corresponde de forma única a una tarjeta o dispositivo de red

---

7.10. P

7.10.1. Protocolo seguro de transferencia de hipertexto

Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto

---

7.11. S

7.11.1. Servicio de mensajería multimedia

Es un estándar de mensajería que le permite a los teléfonos móviles enviar y recibir contenidos multimedia, incorporando sonido, video o fotos

7.10.2. Servicio general de paquetes vía radio

Es un punto de acceso que puede utilizar servicios de comunicación

7.10.3. Sistema de posicionamiento global

Se refiere a un sistema que permite determinar en toda la Tierra la posición de un objeto

7.10.4. Sistema de posicionamiento global

Es una tarjeta inteligente desmontable usada en teléfonos móviles. Almacena de forma segura la clave de servicio del suscriptor usada para identificarse ante la red

7.10.5. Sistema global para las comunicaciones móviles

Es el sistema global para las comunicaciones móviles

7.10.6. Sniffer

Es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador

7.10.7. Secure Sockets Layer

Es la tecnología de seguridad estándar para establecer un enlace encriptado entre un servidor web y un navegador.

7.11. T

7.11.1. TransportLayer Security

Proporciona privacidad e integridad de datos entre dos aplicaciones que se comunican. A diferencia de SSl, este protocolo admite algoritmos más nuevos y más seguros.

7.12. O

7.12.1. Open Source

Se refiere a código abierto y es un modelo de desarrollo de software basado en la colaboración abierta

---

7.13. U

7.13.1. Unidad Aritmética Lógica

Es un circuito digital que calcula operaciones aritméticas y operaciones lógicas entre valore de los argumentos

7.13.2. Unidad Central de Procesamiento

Hardware que interpreta las instrucciones de un programa informático mediante la realización de las operaciones básicas

---

7.14. W

7.14.1. Wipe Data

Es un algoritmo de eliminación de datos utilizado en aplicaciones anti-robo

---