Instituto Politécnico Nacional

"La Técnica al Servicio de la Patria"

CIC

Centro de Investigación en Computación

Laboratorio de Ciberseguridad

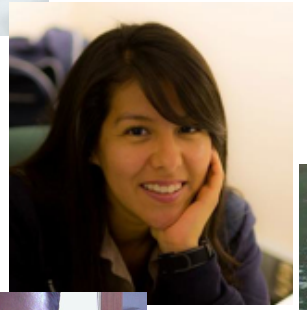
Miembros

Dr. Eleazar Aguirre
SNI C
CIC-IPN

Dr. Raul Acosta
CGSI
CIC-IPN

Dra. Nareli Cruz
SNI 1
CIC-IPN

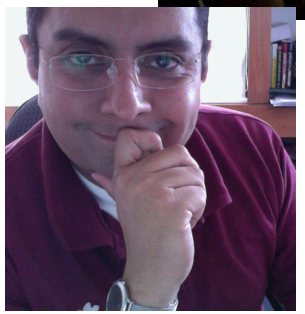
Dra. Gina Gallegos
SNI C
ESIMECU



Dr. Abraham Rodriguez
CIC-IPN /ESIMEZ-IPN

Dr. Ponciano Escamilla
SNI 1
CIC-IPN

Dr. Francisco Rodriguez
SNI 2
CINVESTAV-IPN



Dr. Moisés Salinas
SNI C
CIC-IPN

Propuestas de grandes proyectos

Plataforma para comunicaciones seguras

Detección y Análisis de Malware

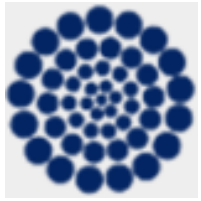
Modelos de Seguridad para cómputo en la nube y BigData

Seguridad para Ciudades inteligentes

Malware e Internet de las Cosas

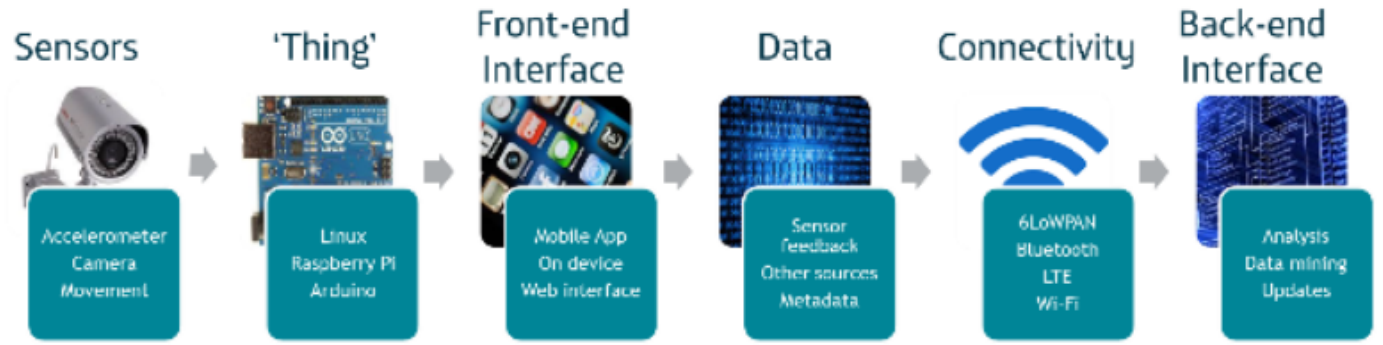
Laboratório de Ciberseguridad, CIC-IPN.

Presenta: Dr. Abraham Rodríguez Mota



El Internet de las Cosas (IoT)

- El IoT promete extender el computo a “cualquier lado, de cualquier forma, en cualquier momento” para “cualquier cosa, cualquier persona, cualquier servicio”.
- Cada persona y cosa tiene una contraparte en el Internet que es localizable, direccionable y leible.
- IoT no debe ser pensada solo como una “Cosa” por si sola.
- Es una colección de tecnologías integradas y presentes para proporcionar vastas aplicaciones específicas y diversas.
- Esto también se refleja en cuan “inteligente” el dispositivo será realmente, desde el “Dumb” o sin conexión, pasando por la inteligencia básica de monitoreo hasta semi autónomos, donde el dispositivo realizará algunas acciones de forma automática como una respuesta a la entrada hasta la autonomía total del dispositivo IoT, recolectando y procesando datos, tomando acción mientras se comunica automáticamente con otros dispositivos.



Partes constituyentes de un ecosistema IoT.
Fuente: https://www.elevenpaths.com/wp-content/uploads/2015/10/TDS_Insecurity_in_the_IoT.pdf

El Internet de las Cosas (IoT)

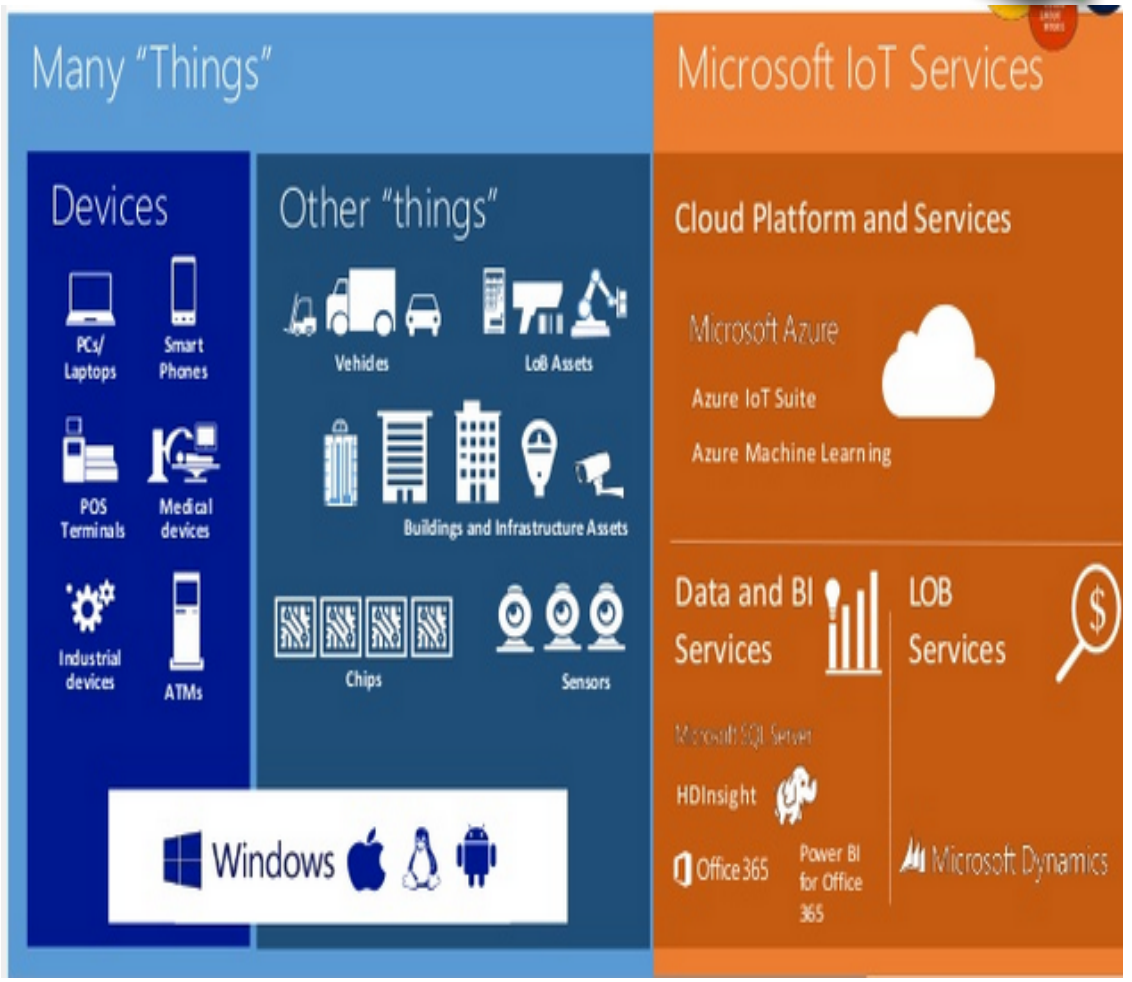
- Conforme los dispositivos pasan por este ciclo de maduración del IoT la exposición a riesgos y el potencial impacto de un incidente de seguridad se incrementa con la capacidad.

- Naturaleza altamente distribuida
- Uso de tecnologías frágiles, como dispositivos incrustados de funciones limitadas en áreas públicas, crea enlaces débiles que las entidades maliciosas pueden explotar.

- Diferentes factores pueden conducir a riesgos de seguridad:
  - Defectos constantes.
  - Bugs.
  - Errores en la lógica.

Dispositivo Físico (La “Cosa”)

- Los dispositivos pueden tener un amplio rango de formas, pueden ser cualquier “cosa”.
- Pueden conducir únicamente una tarea o agendar distintas tareas.
- Son una plataforma estándar de computo técnicamente capaz de operar fuera de los parámetros de diseño.
- Los últimos avances en computación distribuirán la actividad de procesamiento y pueden ser capaces de reducir significativamente la cantidad de datos transmitidos conforme las capacidades se incrementen.



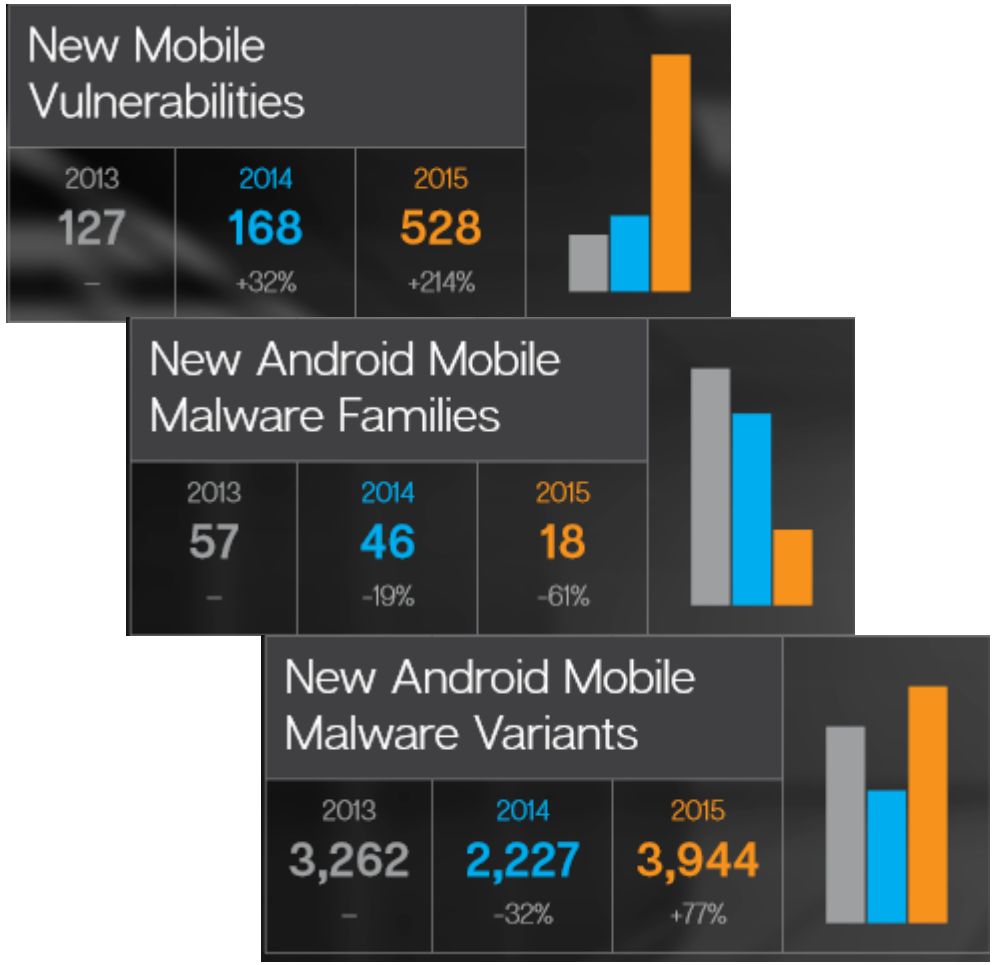
Fuente: http://www.slideshare.net/Codemotion/iot-endtoend-porta-i-tuoi-dati-dal-sensore-al-cloud

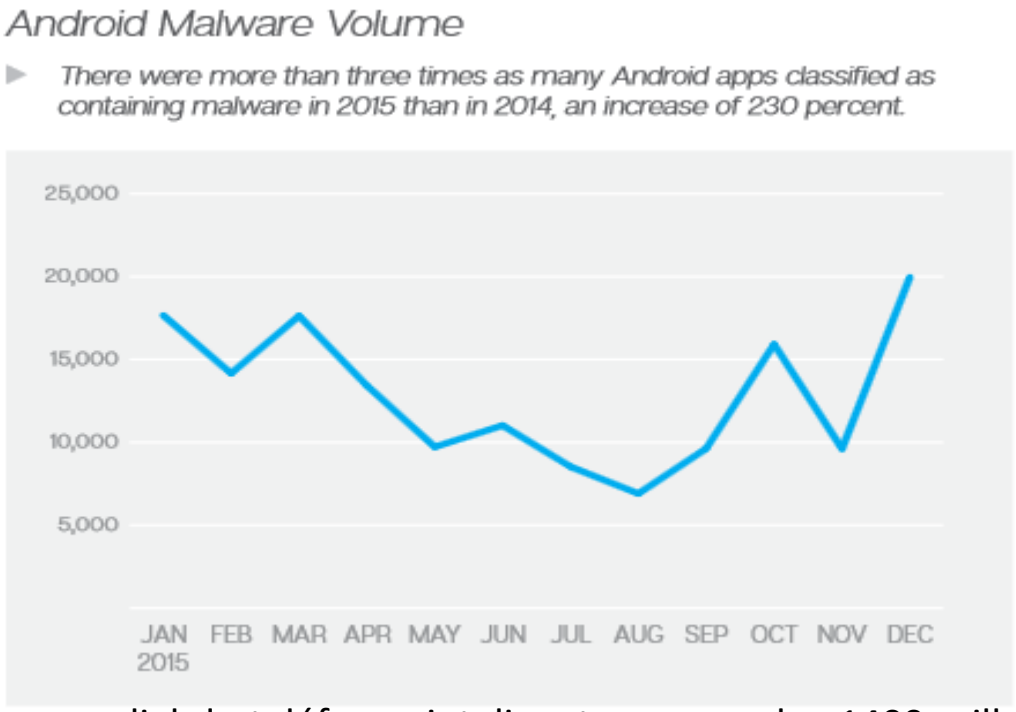
Interface Frontal

- La forma en que el usuario final interactúa con la funcionalidad del dispositivo o servicio puede ser realizado remotamente vía la web o una aplicación móvil, como el control de termostato Google Nest.
- Alternativamente pueden ser incrustados dentro del mismo dispositivo, como un refrigerador inteligente.
- La administración proporciona sus propios retos y en el Mercado para casas comienzan a aparecer soluciones que proporcionan una sola interface con la cual se controlan diversos dispositivos IoT dentro del hogar.

Fuente: http://www.ipwatchdog.com/2015/08/15/synthos-generates-operating-system-code-for-iot-devices-reducing-development-costs/id=59945/

El lugar de Android en el Mercado





La venta mundial de teléfonos inteligentes supero los 1400 millones en 2015, por arriba del 10 porciento de las 1300 billones de unidades vendidas en el año previo, de acuerdo a IDC's Worldwide Quarterly Mobile Phone Tracker (Enero 27, 2016). Cinco de cada 6 teléfonos nuevos utilizaban Android, contra uno de cada siete empleando Apple iOS (Smartphone OS Market Share, 2015, Q2).

Fuente: Symantec. Internet Security Threat Report, Abril 2016
https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Política de Seguridad de Android

- Android protege las aplicaciones y datos a través de una combinación de dos mecanismos de enforzamiento, uno al nivel de Sistema y otro al nivel de Comunicación entre Procesos (IPC).

- En el caso general, cada aplicación se ejecutan con una identidad única de usuario, lo que le permite a Android limitar el potencial de daño.

- IPC no están limitados por el usuario o los limites de los procesos.

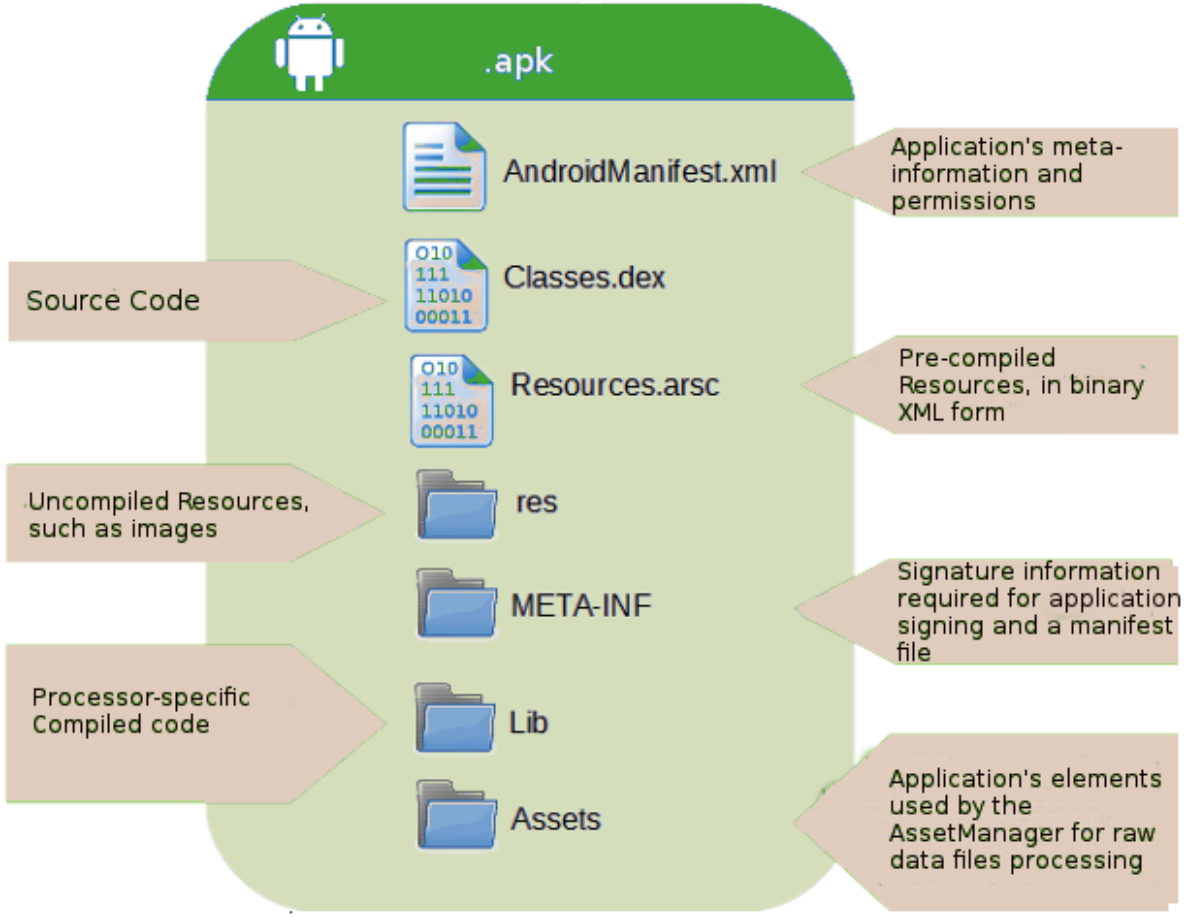
- Todas las etiquetas de permisos son establecidas al momento de la instalación de una aplicación y no se pueden modificar a menos de que se reinstale.

AndroidManifest.xml

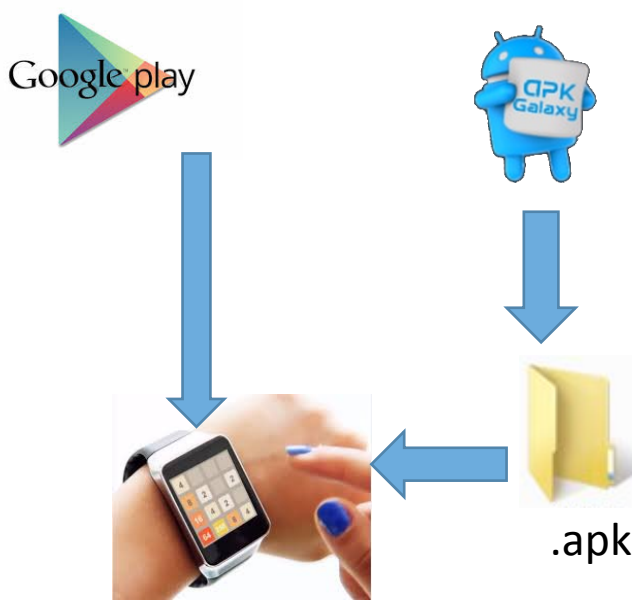
Un componente inicia un IPC

- Observa las etiquetas de permisos asignadas dentro de las aplicaciones.
- Permite el establecimiento de IPC si la etiqueta apropiada esta presente.

Elementos de una aplicación Android



El proceso de construcción de Android proporciona configuraciones de proyectos y construcción de módulos de manera que los módulos de Android son compilados y empaquetados en archivos .apk.

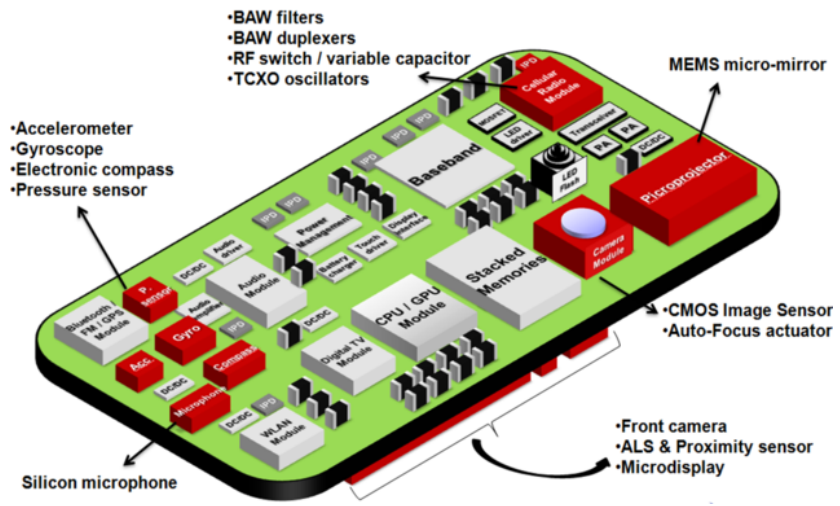


Amenazas en Android

- Las vulnerabilidades en dispositivos móviles continúan evolucionando conforme los dispositivos con Android continúan siendo más atractivos para los atacantes.
- Los dispositivos móviles contienen sensores y actuadores que históricamente no se encuentran en computadoras personales o servidores, los cuales recolectan y transmiten información privada sobre el usuario del dispositivo.

- La lista de sensores que pueden revelar información sensible incluye:
  - Cámaras, micrófonos, acelerómetros, sensores de gravedad, sensores de vectores de rotación, giroscopios, magnetómetros, sensores GPS , Near-Field Communication (NFC), sensores de luz, chips de seguimiento M7, barómetros, termómetros, podómetros, monitores cardiacos, y sensores de huellas digitales [2].

- Las vulnerabilidades de violación de la privacidad que ocurren en dispositivos móviles pueden conducir a la revelación de la **ubicación, imágenes sensibles, datos entrados por medio del teclado o a través de la pantalla.**
- Mientras que los teléfonos móviles pueden ser utilizados para ver, manipular y almacenar datos localmente, estos dispositivos permiten al usuario interactuar con un mundo de recursos interconectados. Mediante los protocolos de comunicación, tanto los datos sensibles como los inócuos son comunicados entre servicios remotos en diferentes equipos.



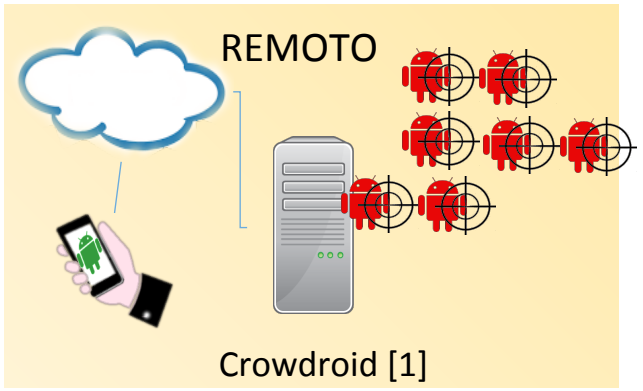
Fuente: https://www.prlog.org/10792126-mems-sensors-for-smartphones-report.html

Amenazas en Android

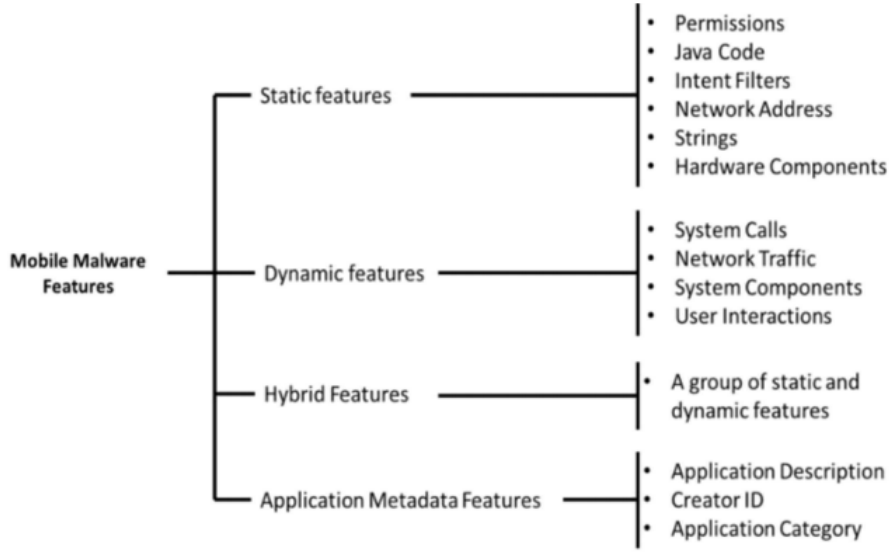
- Android Wake on Lan (AWOL)
- Passwords débiles
- Datos expuestos
- SMShing
- Navegación no segura
- Aplicaciones Intrusivas
- Aplicaciones re-empaqueadas y fraudulentas
- Android Malware
- Anti-Malware Falsos
- Falta de visibilidad y Control

Fuente: https://www.prlog.org/10792126-mems-sensors-for-smartphones-report.html

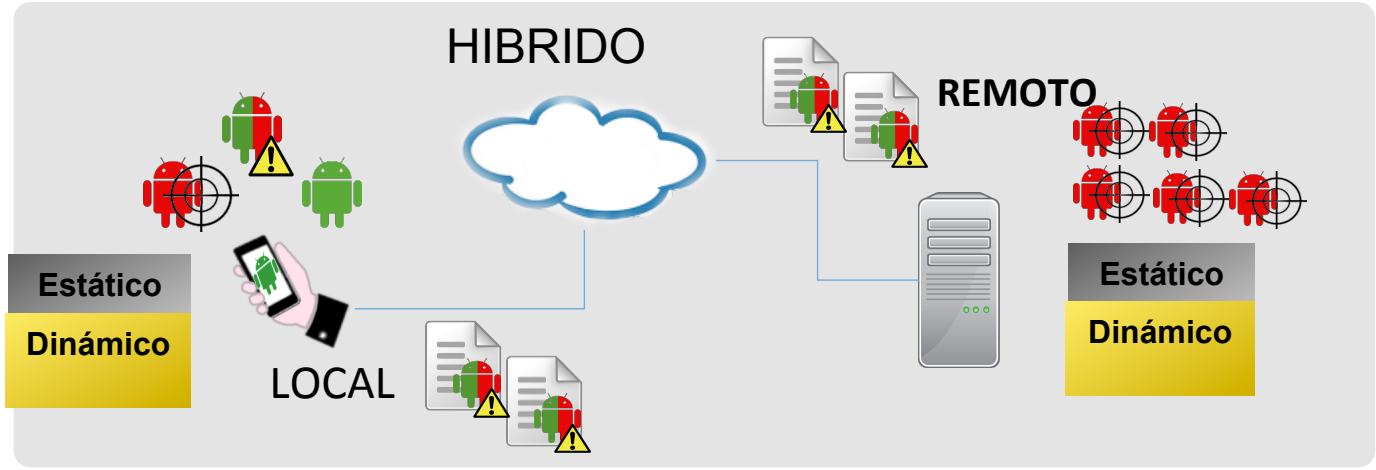
Análisis de Malware en Android



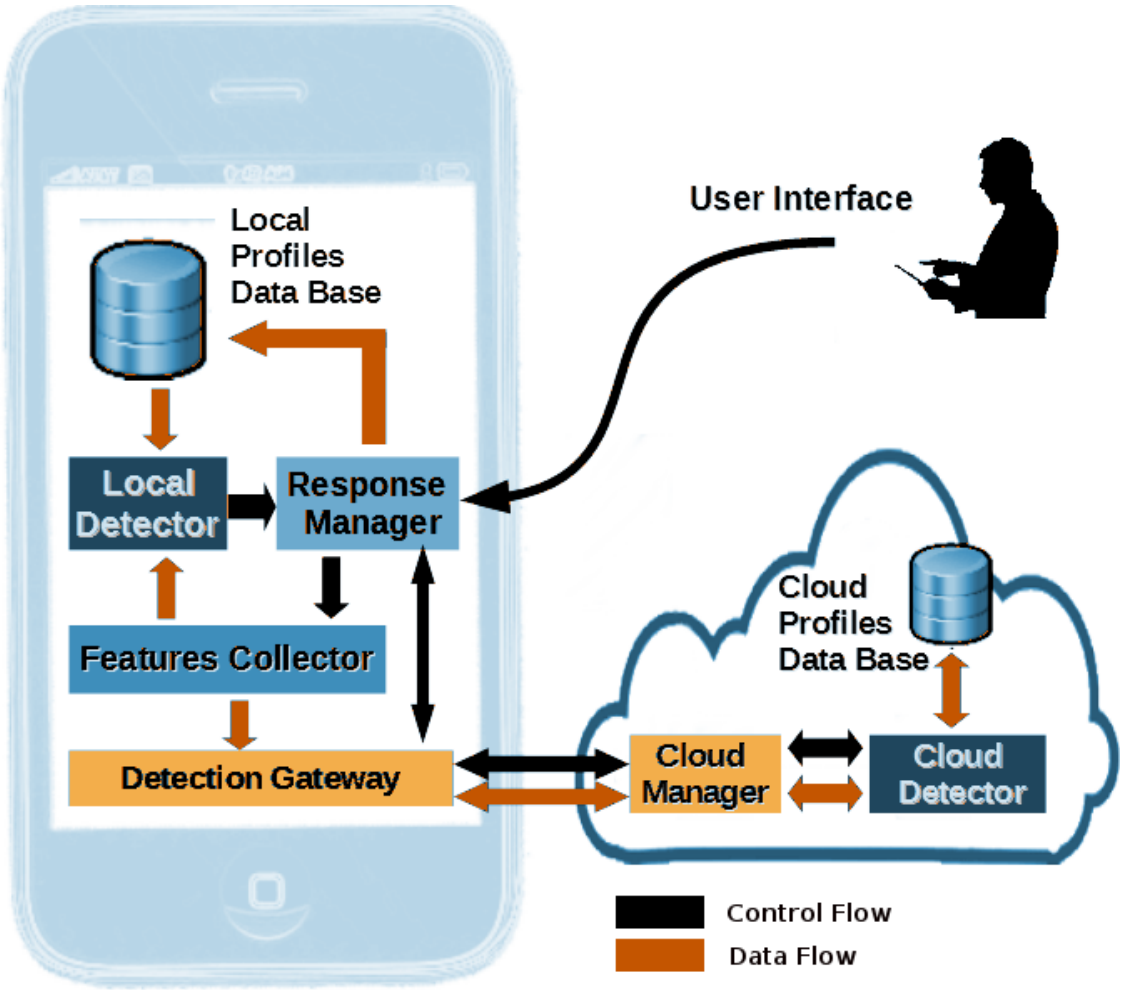
Crowdroid [1]
CloneDroid[2]
ParanoidAndroid[3]

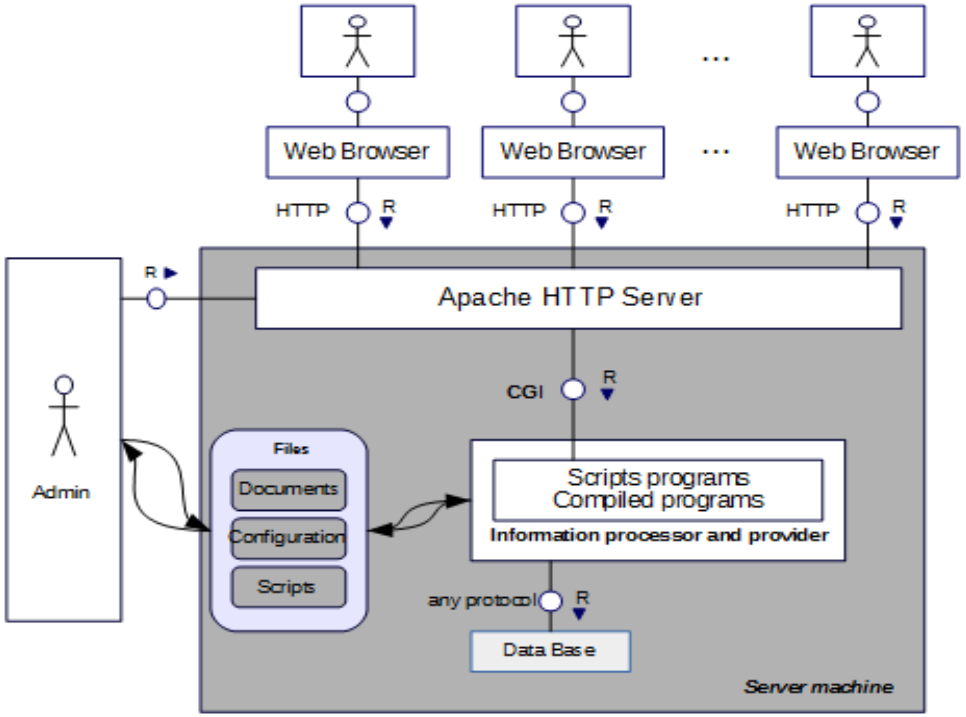


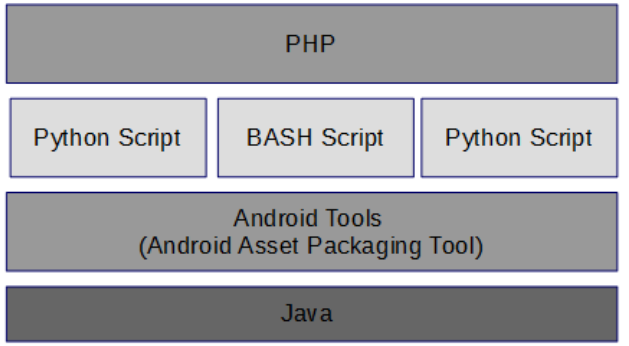
- La mayoría de los sistemas actuales empleados para la detección de código malicioso se basan ampliamente en firmas y técnicas de análisis estático.



Garmdroid y el análisis 2-híbrido





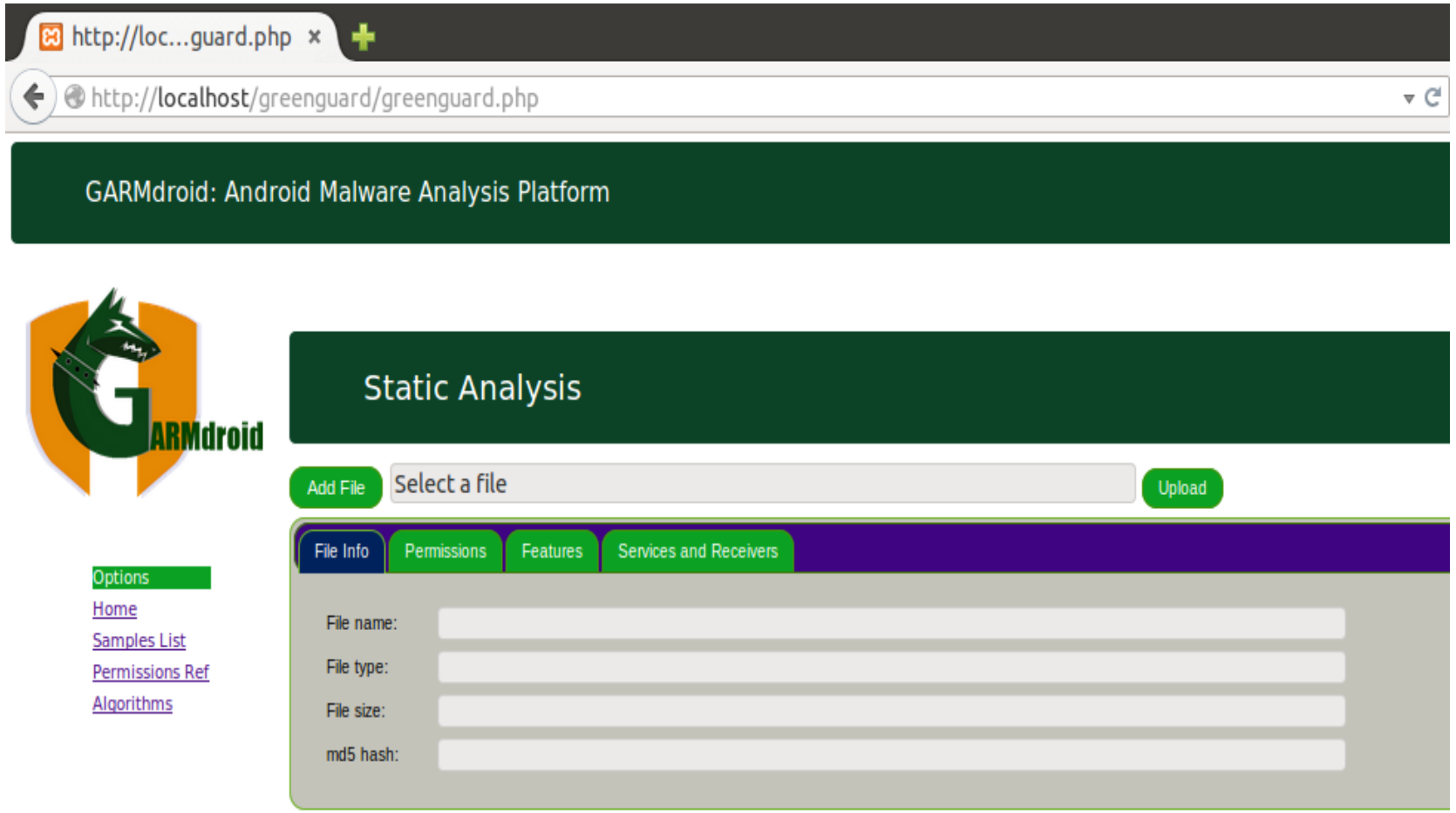


Interface de Garmdroid

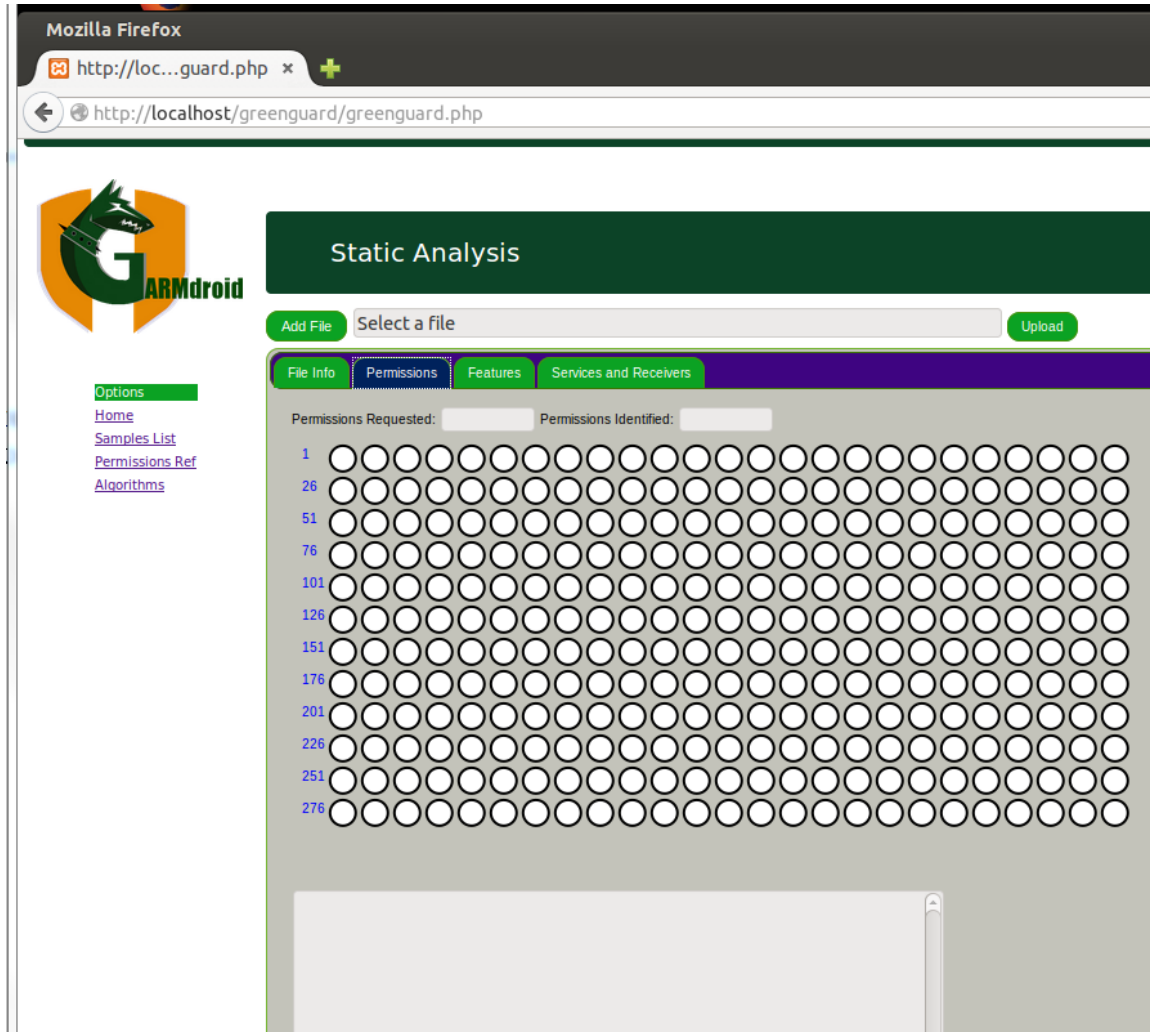
GARM + ANDROID = GARMDROID

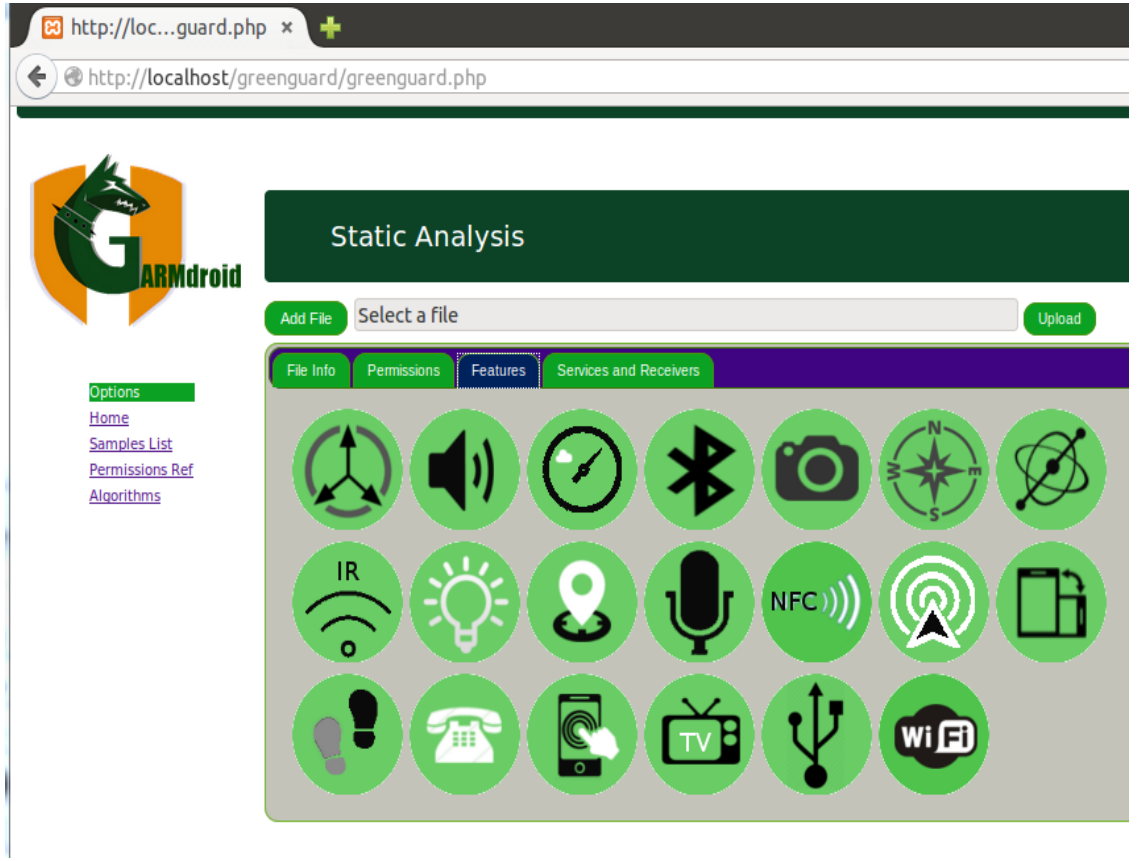
Garm en la mitología Nórdica es el nombre dado a un perro guardián de las puertas del infierno.

www.garmdroid.org

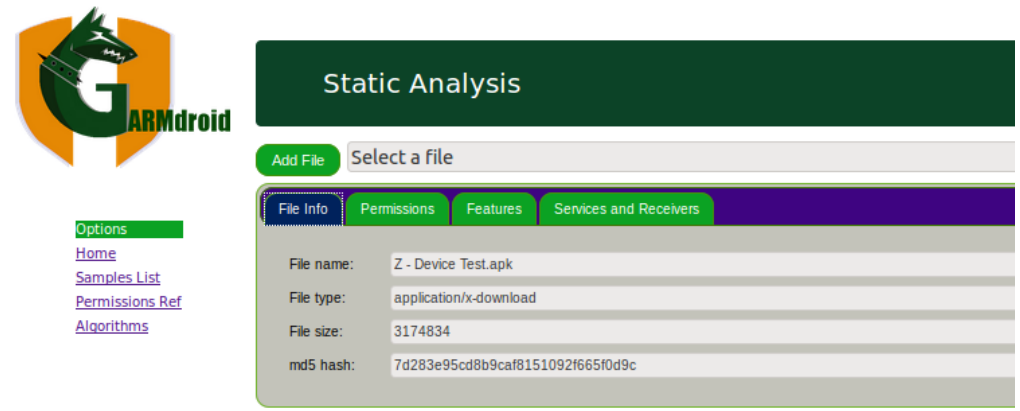


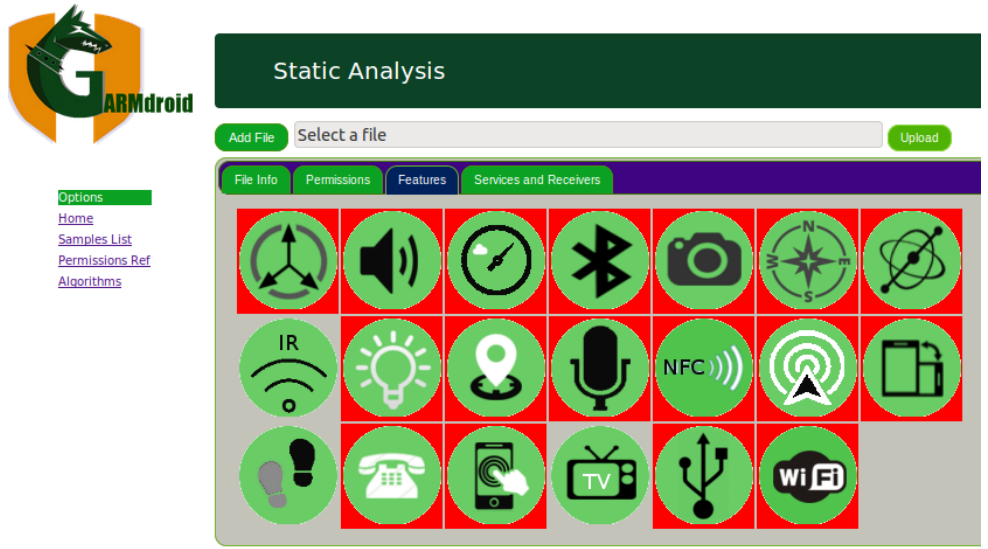
Interface de Garmdroid

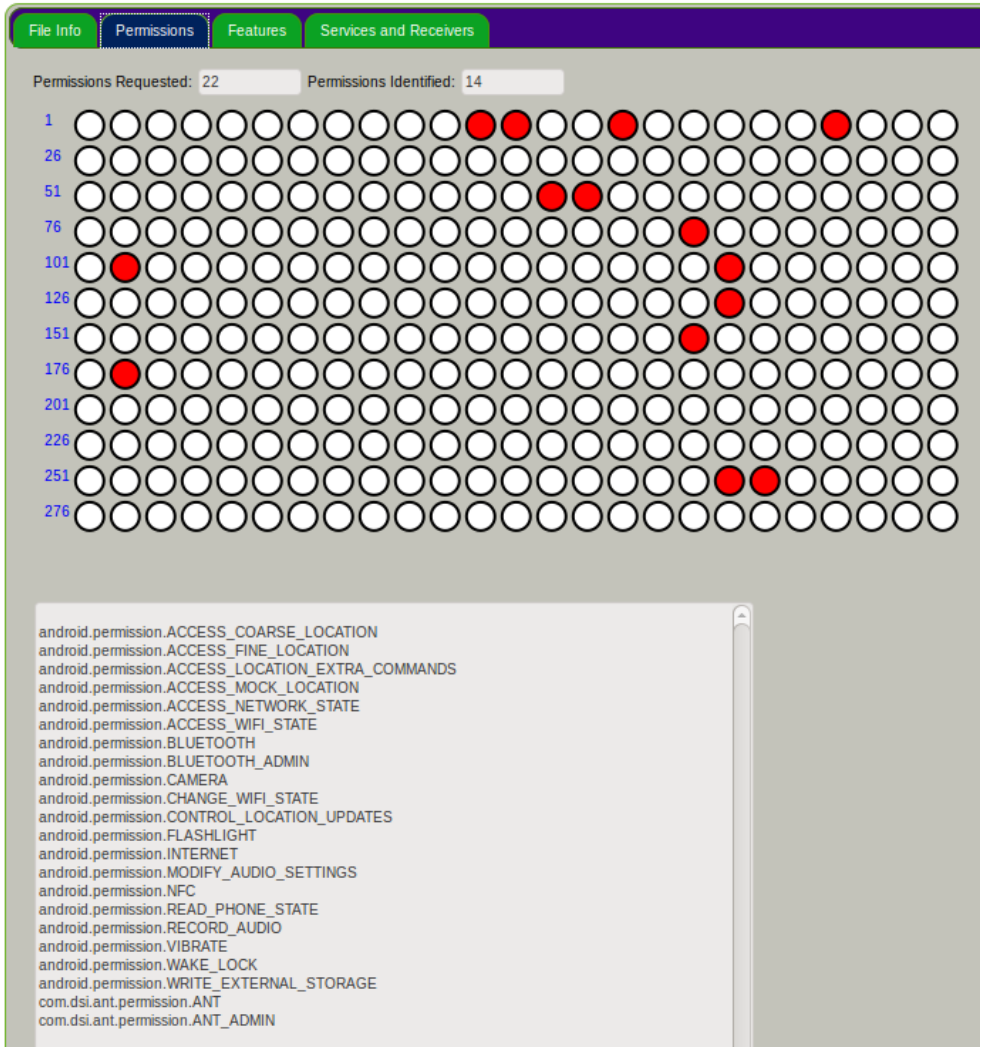




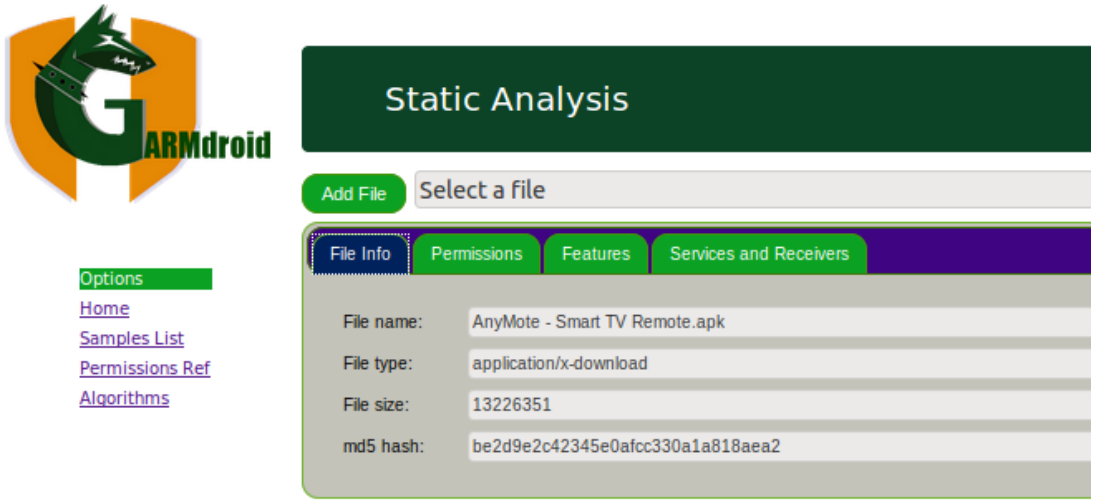
Muestra de una aplicación de prueba de Hardware

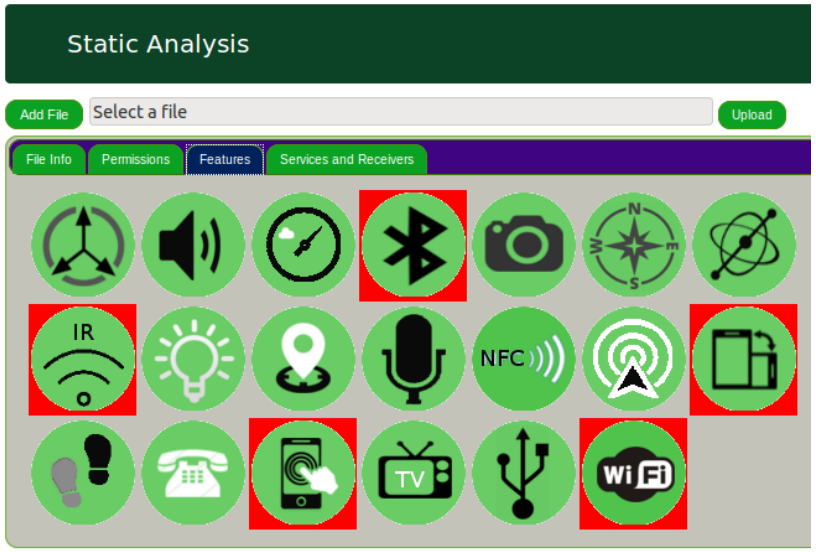


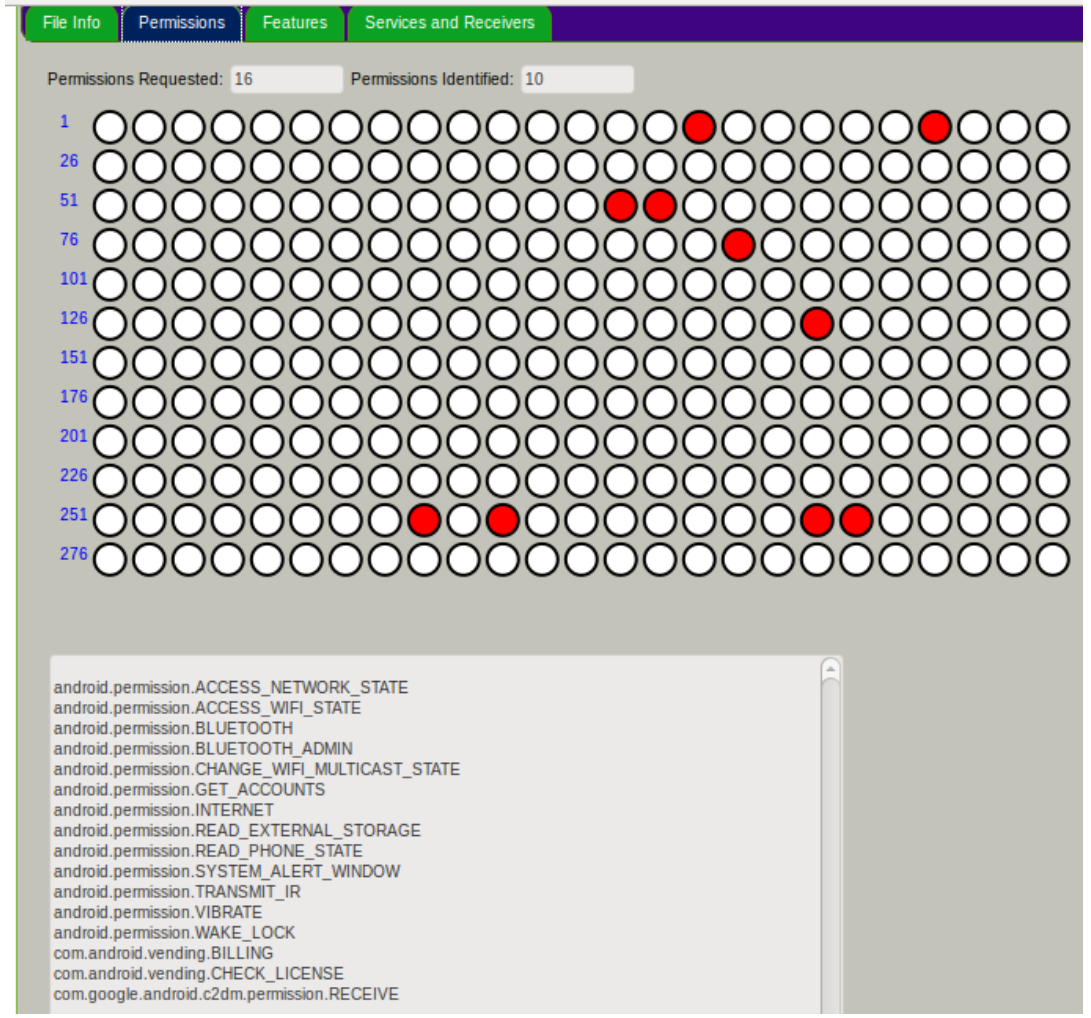




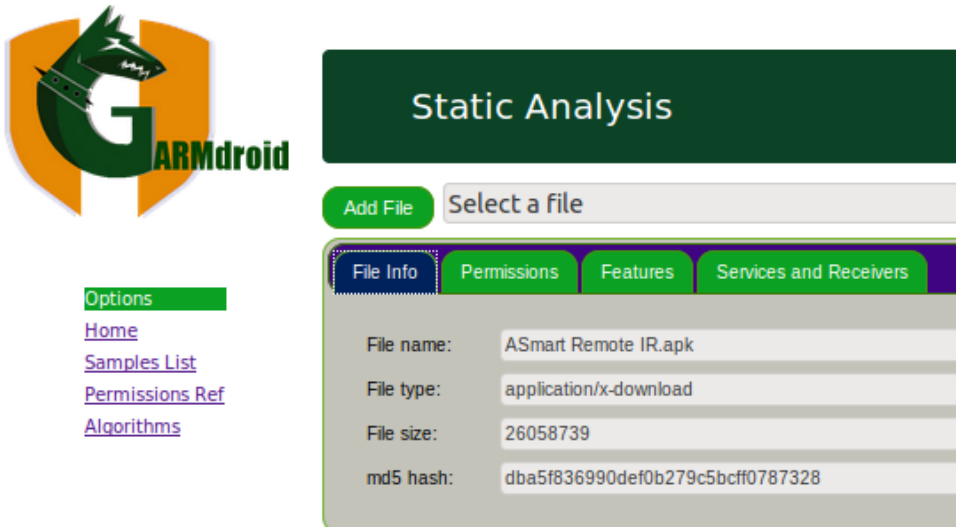
Muestra de aplicación de Control Remoto Infrarojo (1)

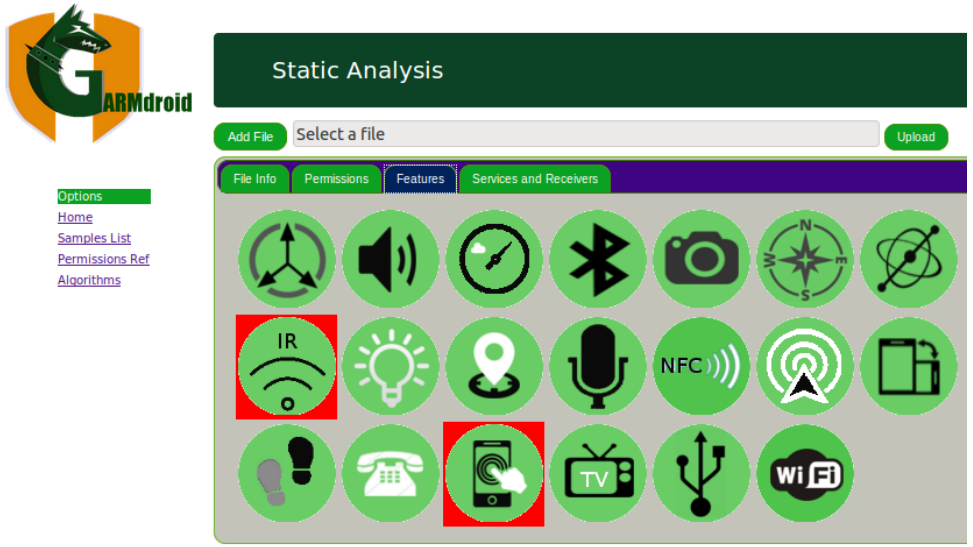


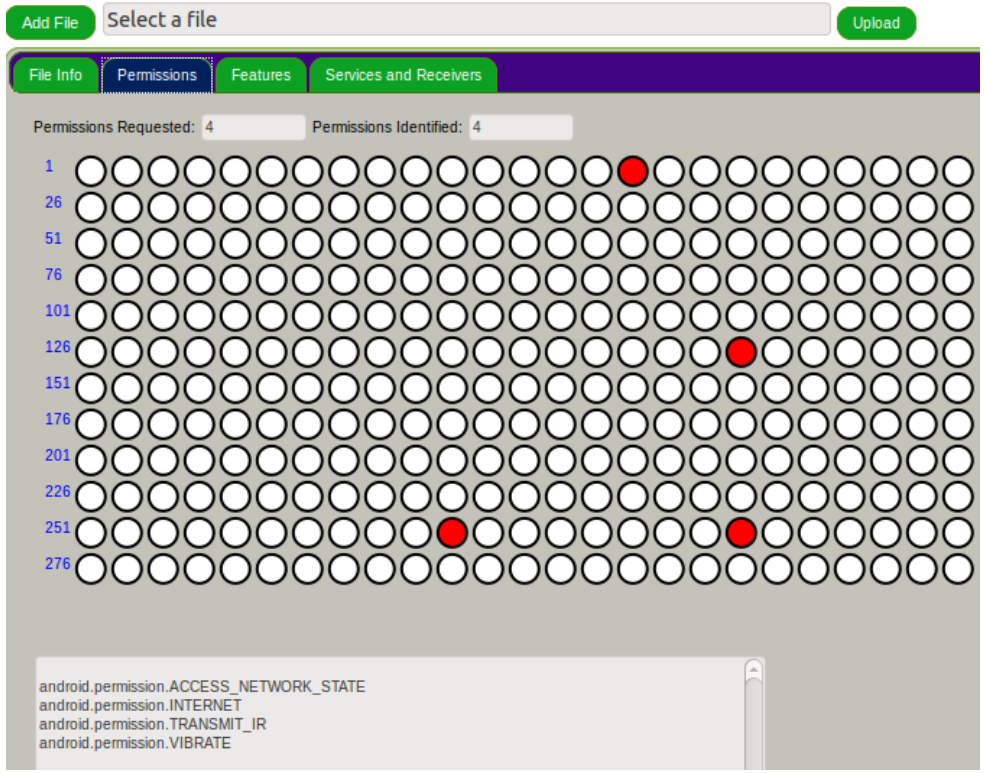




Muestra de aplicación de Control Remoto Infrarojo (2)







Muestra de aplicación de linterna

Options
Home
Samples List
Permissions Ref
Algorithms

Static Analysis

Add File | Select a file

File Info | Permissions | Features | Services and Receivers

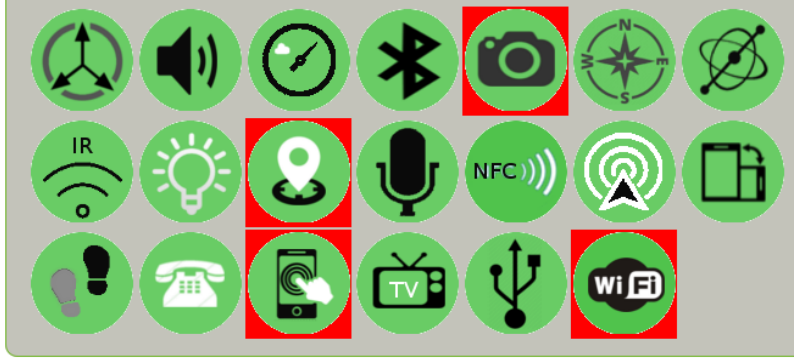
File name: com.mobusi.linternapotenteconsonidosemergencia-1230.apk
File type: application/x-download
File size: 9945130
md5 hash: 1172c7d76a5d7ea7ae89867547bd2bec

Options
Home
Samples List
Permissions Ref
Algorithms

Static Analysis

Add File | Select a file | Upload

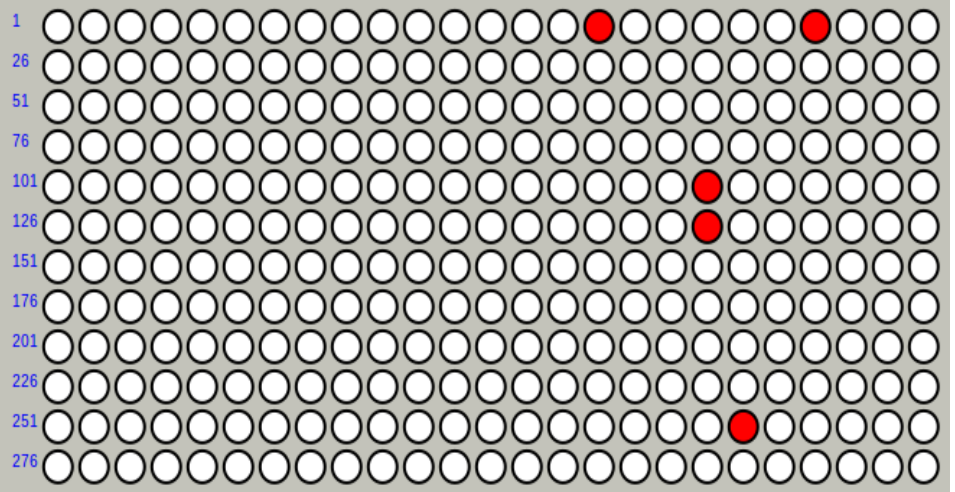
File Info | Permissions | Features | Services and Receivers



Add File | Select a file | Upload

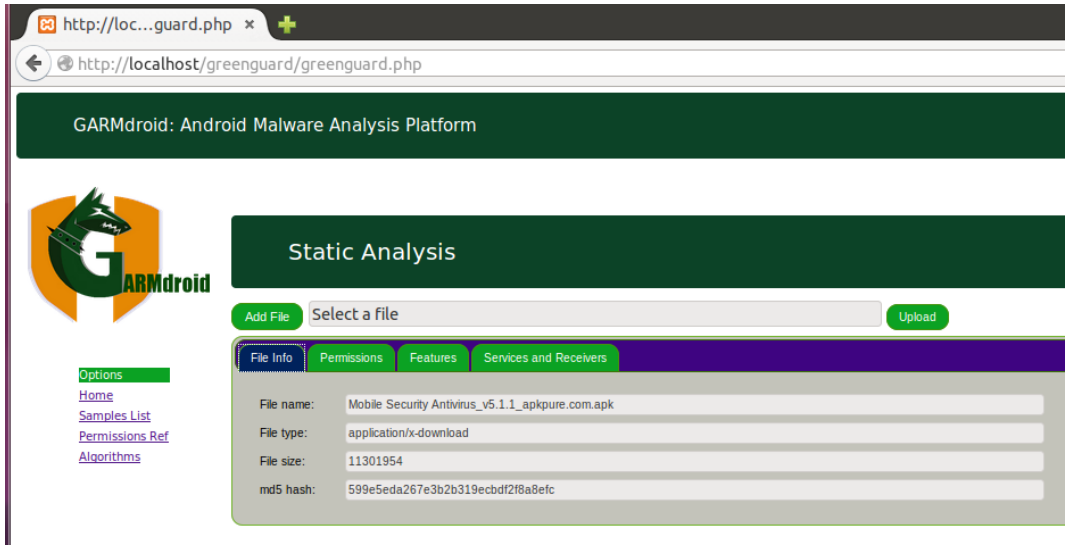
File Info | Permissions | Features | Services and Receivers

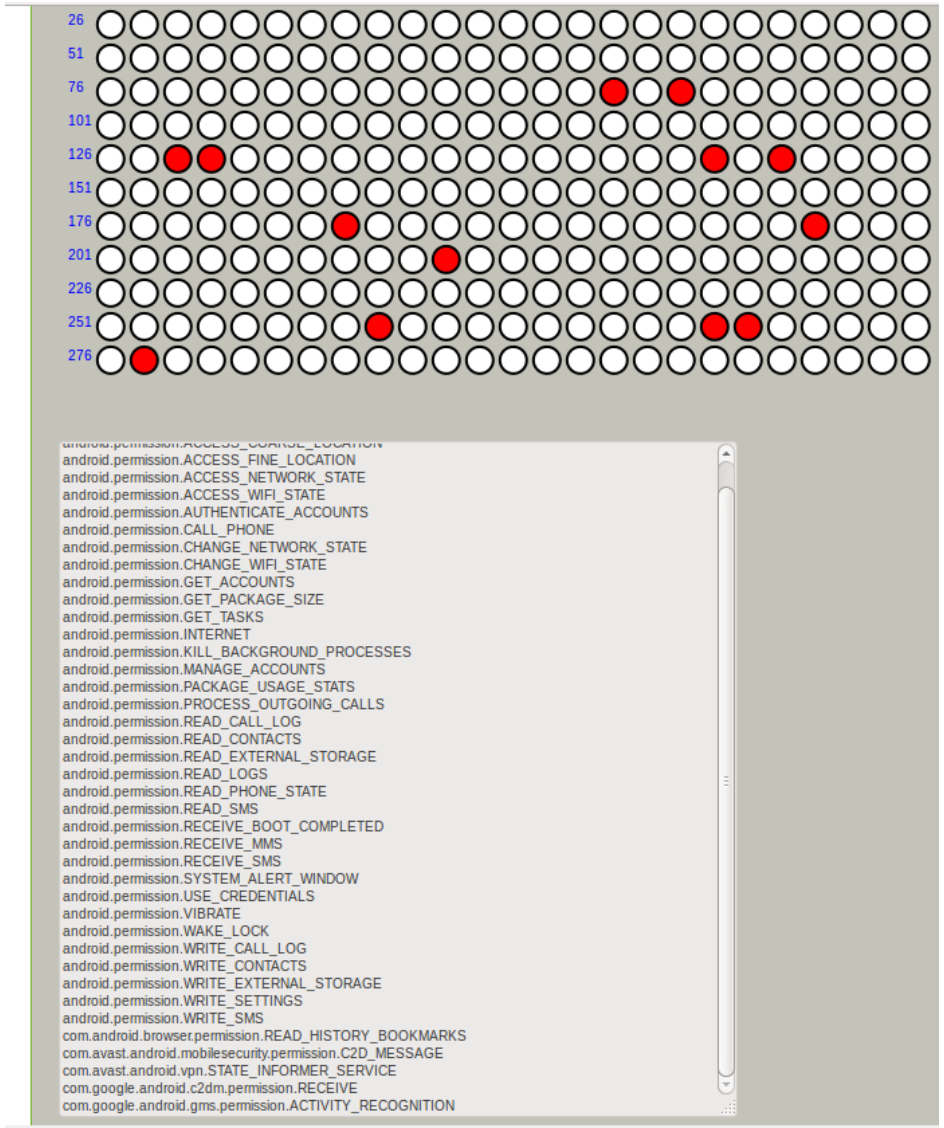
Permissions Requested: 11 Permissions Identified: 5



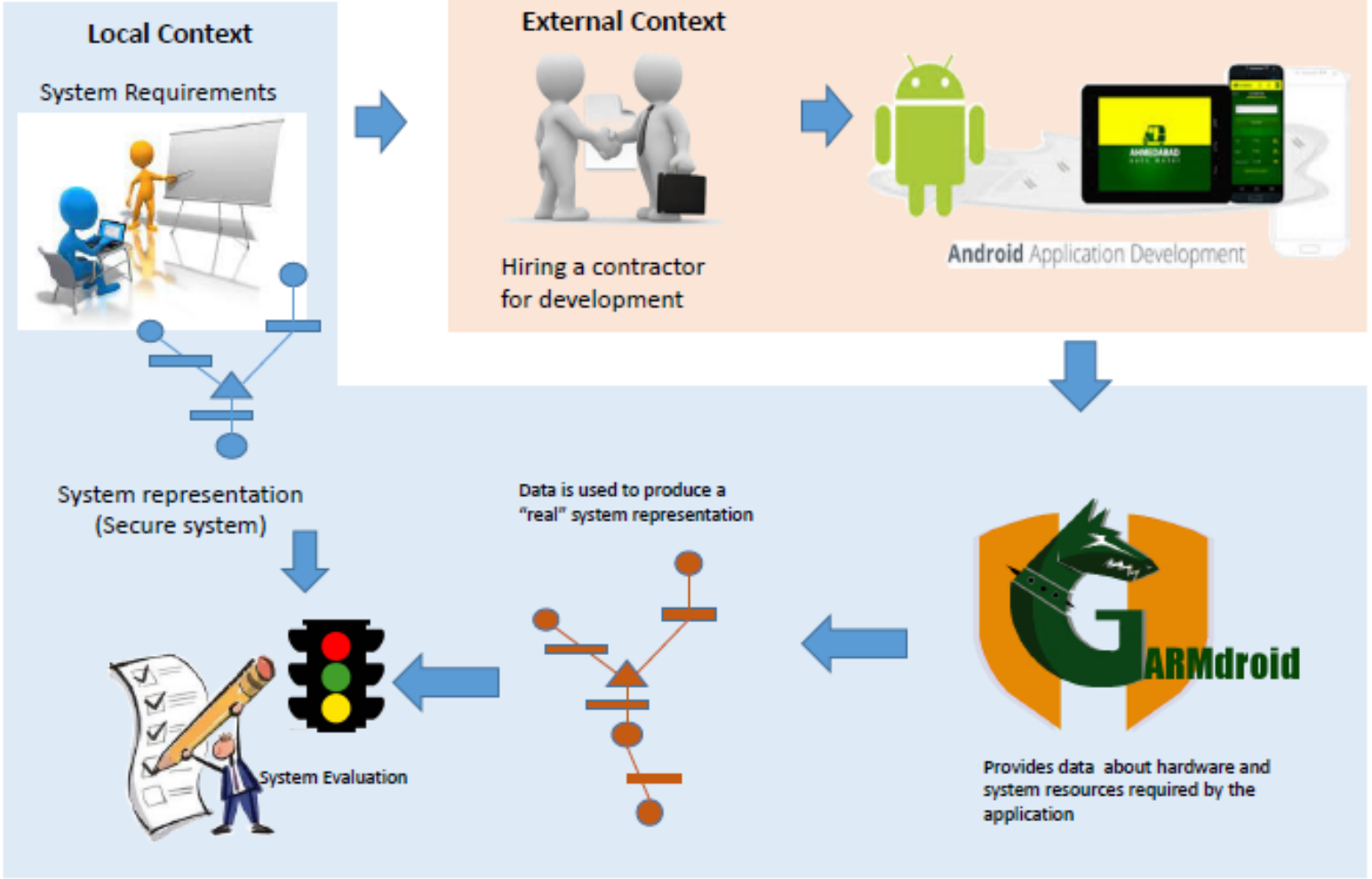
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.CAMERA
android.permission.FLASHLIGHT
android.permission.GET_ACCOUNTS
android.permission.INTERNET
android.permission.USE_CREDENTIALS
android.permission.WAKE_LOCK
android.permission.WRITE_EXTERNAL_STORAGE
com.google.android.c2dm.permission.RECEIVE

Muestra de aplicación Antivirus





Trabajos Futuros



UNIVERSITY OF OXFORD

IPN

Conclusiones

- Las tendencias actuales en el uso de dispositivos móviles representa un medio muy llamativo y remunerativo para los desarrolladores de Malware.
- Con el advenimiento del IoT, no solo conlleva beneficios sino también se presentan mayores vulnerabilidades y amenazas de seguridad.
- Esta situación representa una tendencia alarmante debido a la naturaleza de los datos que se procesan, almacenan y comparten en los diversos dispositivos “Cosas” que hacen uso de los recursos y servicios que el IoT brinda.
- Sin embargo, desde el punto de vista de investigación, se observa un nicho de oportunidades de amplias dimensiones.
- Nuestras investigaciones han generado interés en diversos sectores de la industria y la academia.

¿Preguntas?