Jornadas “Espacios de Ciberseguridad”

Malware en Android

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

NATIONAL CYBERSECURITY INSTITUTE OF SPAIN

Índice

INCIBE - ¿Qué es?

El Instituto Nacional de Ciberseguridad de España (**INCIBE**) es una sociedad dependiente del Ministerio de Industria, Energía y Turismo (**MINETUR**) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (**SETSI**).

INCIBE es la entidad de referencia para el desarrollo de la **ciberseguridad** y de la **confianza digital** de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos (Agenda Digital para España, aprobada en Consejo de Ministros el 15 de Febrero de 2012).

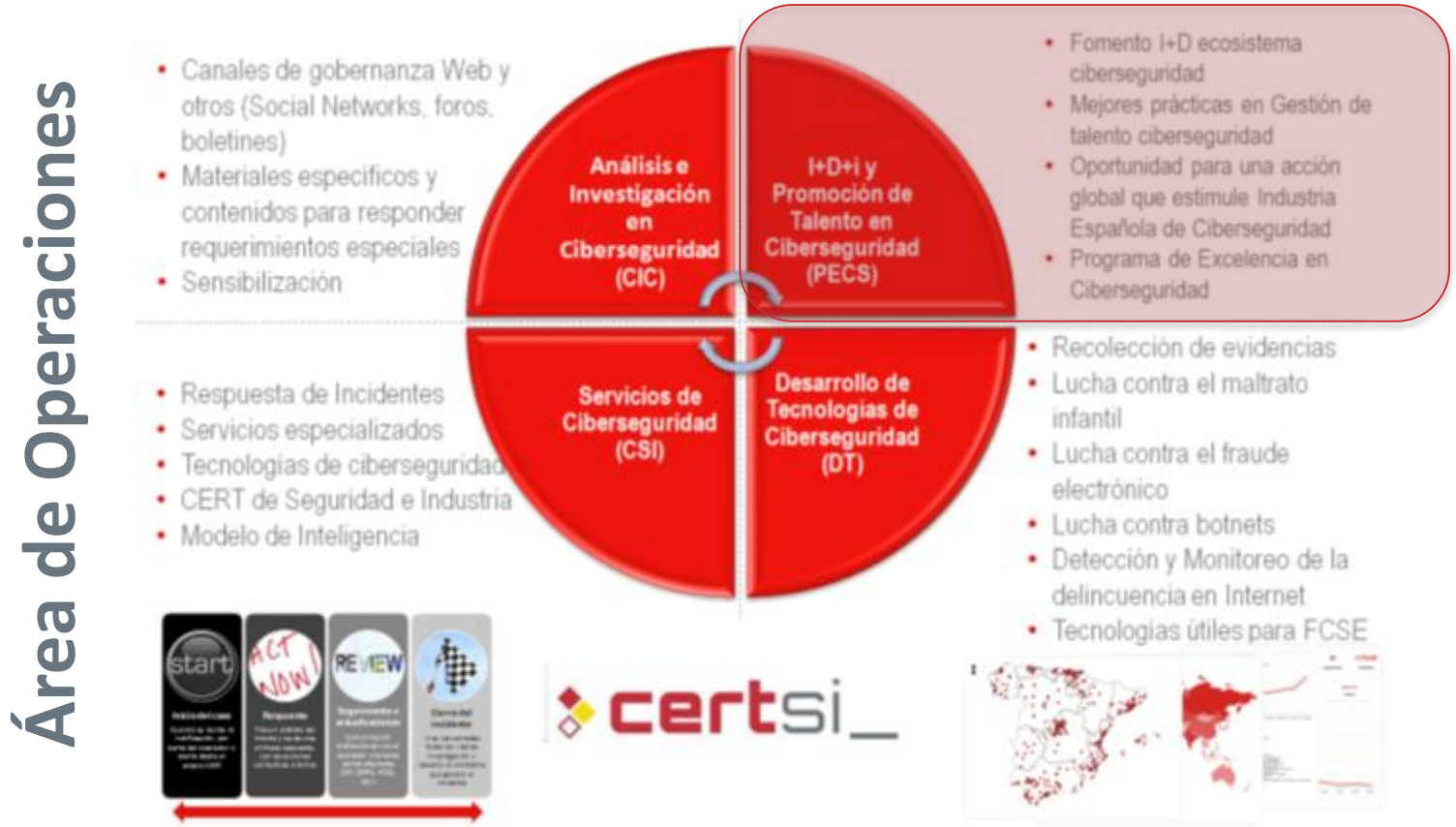
Como **centro de excelencia**, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia , INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

www.incibe.es

INCIBE - ¿Qué es?

Pilares fundamentales sobre los que se apoya la actividad de INCIBE

- **Prestación de servicios** de protección de la privacidad, prevención y reacción a incidentes en ciberseguridad
- **Investigación** generación de inteligencia y mejora de los servicios
- **Coordinación** colaboración con entidades públicas y privadas, nacionales e internacionales



I+D+i y Promoción del Talento en Ciberseguridad

Fomento del Ecosistema de I+D+i en Ciberseguridad

"…INCIBE como Centro de Excelencia impulsa el ecosistema nacional de I+D+i en Ciberseguridad…"

Enfoque **INTEGRADO** de la I+D+i

- Análisis y diagnóstico de la Investigación en Ciberseguridad (**Conocimiento** de las actividades que se llevan a cabo, contar con los **investigadores** como activo principal y tener **infraestructuras**)
- Red de Centros de Excelencia en I+D+i en Ciberseguridad (Plan Director e inteligencia colectiva) a través del lanzamiento de la **Agenda Estratégica Nacional I+D+I en Ciberseguridad**

Mejor **ENFOQUE** y coordinación

- Agenda Estratégica Nacional I+D+i en Ciberseguridad (programas nacionales I+D)
- Agenda Estratégica Internacional I+D+I Comisión Europea (**NIS WG3**) (programa internacional H2020)

Resultados **orientados a Negocio**

- SPIN-OFF / SPIN-UP.
- Lanzaderas / incubadoras / aceleradoras de START-UPs.
- Capital semilla / Capital riesgo (VC).
- Transferencia de conocimiento a la industria

(capital humano investigador y adquisición de patentes).

Enfoque basado en la **INTERNACIONALIZACIÓN** desde el inicio

I+D+i y Promoción del Talento en Ciberseguridad

Mejores prácticas en la Gestión del Talento en Ciberseguridad

"…INCIBE como Centro de Excelencia impulsa la alta capacitación de profesionales en el ámbito de la Ciberseguridad"

Enfoque **INTEGRADO**

- Itinerarios educativos en Ciberseguridad (alineado con la demanda del sector).
- Coherente a todos los niveles (FP, Grado y Máster y Pre-doctorales y Post-doctorados).
- Iniciativas para la gestión de talento: **atracción, detección, promoción y retención**.

Mejor **ENFOQUE**

- Análisis del GAP entre los itinerarios educativos vs. oferta formativa vs. Iniciativas para la gestión del talento.
- Acciones:
  - **Detección**: Retos tipo pruebas de habilidad.
  - **Atracción**: Formación avanzada y ponentes / premios / reconocimientos / ofertas de empleo.
  - **Promoción**: Reorientación / Nuevos Contenidos prácticos (aspectos técnicos en profundidad para todos los itinerarios educativos) / Formación para jóvenes en ciberseguridad ("Espacios" de Ciberseguridad).
  - **Atracción / Retención**: Financiación de apoyo una vez identificado el talento.

Enfoque basado en la **INTERNACIONALIZACIÓN** desde el inicio buscando su residencia en España

I+D+i y Promoción del Talento en Ciberseguridad

Oportunidad para una acción global que estimule la Industria Española de Ciberseguridad

"…INCIBE como Centro de Excelencia impulsa la competitividad de la Industria nacional de Ciberseguridad en base a un modelo de colaboración público-privada (PPP): Polo de Ciberseguridad …"

Enfoque **INTEGRADO**

- Potenciar el tejido empresarial español en ciberseguridad.
- Renovar la imagen del sector.
- Guiar la innovación y comercialización de nuevos productos/servicios a la demanda nacional/internacional.
- Mejorar el posicionamiento y la comercialización de la industria de la ciberseguridad española.
- Aumentar la actividad productiva competitiva de los participantes a nivel internacional.

Mejor **ENFOQUE**

- Facilitar un **pensamiento estratégico conjunto** para identificar ventajas competitivas y diferenciación.
- Definición de **acciones colectivas** para abordar los desafíos estratégicos.
- **Priorización** e **implementación rápida** de las acciones identificadas.
- Fomento de una **colaboración público-privada** con los principales actores de la industria.
- Definición de un **modelo de gobierno** que permite una **sostenibilidad** a largo plazo.

Resultados orientados a NEGOCIO

- Acceso a nuevos mercados.
- Innovación.
- Demanda sofisticada, certificación y la concienciación.
- Financiación.

Índice

Introducción a la ciberseguridad

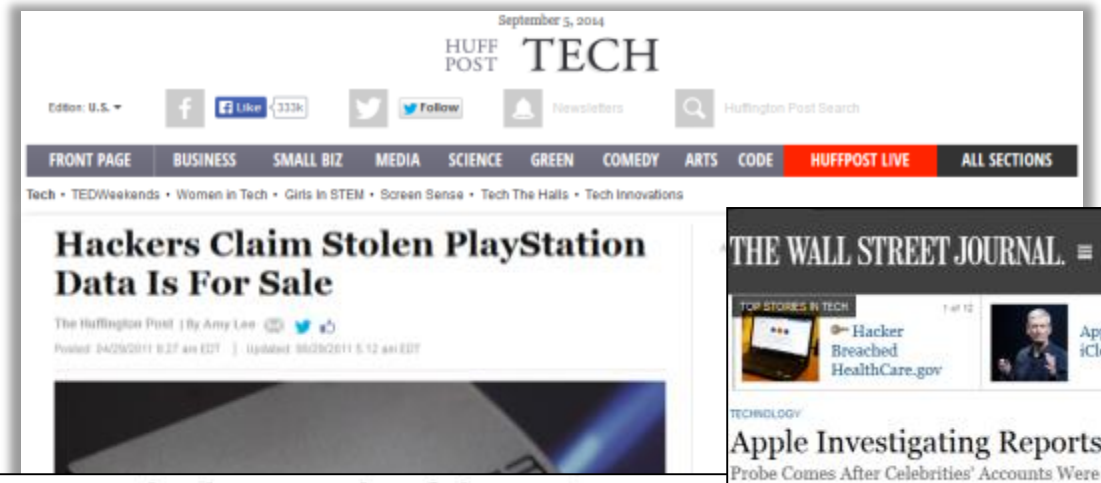
Evolución de las Tecnologías de la Información

- La **información** es uno de los principales activos de una empresa.
- Las empresas almacenan y gestionan la información en los **Sistemas de Información**.
- Para una empresa resulta fundamental proteger sus Sistemas de Información para que su información esté a salvo. Dificultades:
  - El entorno donde las empresas desarrollan sus actividades es cada vez más complejo debido al desarrollo de las tecnologías de información y otros factores del entorno empresarial
  - El perfil de un ciberdelincuente de un sistema informático ha cambiado radicalmente. Si bien antes los objetivos podían ser más simples (acceder a un sitio donde nadie antes había conseguido llegar) en la actualidad los atacantes se han percatado de lo importante que es la información y sobre todo de lo valiosa que puede llegar a ser.

- Es fundamental poner los medios técnicos y organizativos necesarios para garantizar la seguridad de la información. Para lograrlo hay que garantizar la **confidencialidad**, **disponibilidad** e **integridad** de la información.

Introducción a la ciberseguridad

Casos notorios



Introducción a la ciberseguridad

Seguridad de la Información

La seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información:

- La **confidencialidad** es la propiedad de prevenir la divulgación de información a personas no autorizadas.
- La **integridad** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- La **disponibilidad** es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- La **autenticidad**: la información es lo que dice ser o el transmisor de la información es quien dice ser.
- El **no repudio**: Estrechamente relacionado con la Autenticidad. Permite, en caso de ser necesario, que sea posible probar la autoría u origen de una información.

Introducción a la ciberseguridad

Riesgos para los Sistemas de Información

¿Qué son los riesgos en los sistemas de información?

- Las amenazas sobre la información almacenada en un sistema informático.

Ejemplos de riesgos en los sistemas de información

- **Daño físico**: fuego, agua, vandalismo, pérdida de energía y desastres naturales.
- **Acciones humanas**: acción intencional o accidental que pueda atentar contra la productividad.
- **Fallos del equipamiento**: fallos del sistema o dispositivos periféricos.
- **Ataques internos o externos**: hacking, cracking y/o cualquier tipo de ataque.
- **Pérdida de datos**: divulgación de secretos comerciales, fraude, espionaje y robo.
- **Errores en las aplicaciones**: errores de computación, errores de entrada, etc.

Introducción a la ciberseguridad

La figura del HACKER

¿Qué es un hacker?

Experto en seguridad informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

¿Qué tipos de hackers existen en función de los objetivos que tienen?

Black Hat Hackers: Suelen quebrantar la seguridad de un sistema o una red con fines maliciosos.

White Hat Hackers: normalmente son los que penetran la seguridad de los sistemas bajo autorización para encontrar vulnerabilidades. Suelen ser contratados por empresas para mejorar la seguridad de sus propios sistemas.

Gray (Grey) Hat Hackers: Son una mezcla entre los dos anteriores puesto que tienen una ética ambigua. Normalmente su cometido es penetrar en sistemas de forma ilegal para luego informar a la empresa víctima y ofrecer sus servicios para solucionarlo.

Introducción a la ciberseguridad

Clases de ataques

- **Interrupción:** se produce cuando un recurso, herramienta o la propia red deja de estar disponible debido al ataque.
- **Intercepción:** se logra cuando un tercero accede a la información del ordenador o a la que se encuentra en tránsito por la red.
- **Modificación:** se trata de modificar la información sin autorización alguna.
- **Fabricación**: se crean productos, tales como páginas web o tarjetas magnéticas falsas.

Introducción a la ciberseguridad

Técnicas de hacking

- **Spoofing:** se suplanta la identidad de un sistema total o parcialmente.
- **Sniffing:** se produce al escuchar una red para ver toda la información transmitida por ésta.
- **Man in the middle:** siendo una mezcla de varias técnicas, consiste en interceptar la comunicación entre dos interlocutores posicionándose en medio de la comunicación y monitorizando y/o alterando la comunicación.
- **Malware:** se introducen programas dañinos en un sistema, como por ejemplo un virus, un keylogger (herramientas que permiten monitorizar las pulsaciones sobre un teclado) o rootkits (herramientas que ocultan la existencia de un intruso en un sistema).
- **Denegación de servicio:** consiste en la interrupción de un servicio sin autorización.
- **Ingeniería social:** se obtiene la información confidencial de una persona u organismo con fines perjudiciales. El Phishing es un ejemplo de la utilización de ingeniería social, que consigue información de la víctima suplantando la identidad de una empresa u organismo por internet. Se trata de una práctica muy habitual en el sector bancario.
- Adicionalmente existen multitud de ataques como **XSS**, **CSRF**, **SQL injection**, etc.

Introducción a la ciberseguridad

Mecanismos de defensa

Ante esta figura, ¿cómo pueden protegerse las compañías con las nuevas tecnologías?

Los principales sistemas y más conocidos son los siguientes:

- **Firewall:** sistemas de restricción de tráfico basado en reglas.

- **Sistemas IDS / IPS:** sistemas de monitorización, detección y/o prevención de accesos no permitidos en una red.

- **Honeypot:** equipos aparentemente vulnerables diseñados para atraer y detectar a los atacantes, protegiendo los sistemas realmente críticos.

- **SIEM:** sistemas de correlación de eventos y generación de alertas de seguridad.

- **Antimalware:** sistemas de detección de malware informático.

Introducción a la ciberseguridad

Las prácticas del taller se realizan sobre un entorno controlado.

Utilizar las técnicas mostradas en el presente taller sobre un entorno real como Internet, puede ocasionar problemas legales.

Índice

Objetivos del curso

¿Qué vamos a aprender hoy?

- Breve introducción a Android y a su lenguaje de programación, JAVA.
- Arquitectura: funcionamiento de las aplicaciones en Android.
- Fundamentos de la seguridad en Android.
- Malware: Troyanos y gusanos.
- Cómo protegerse adecuadamente.

¿Cómo lo vamos a aprender?

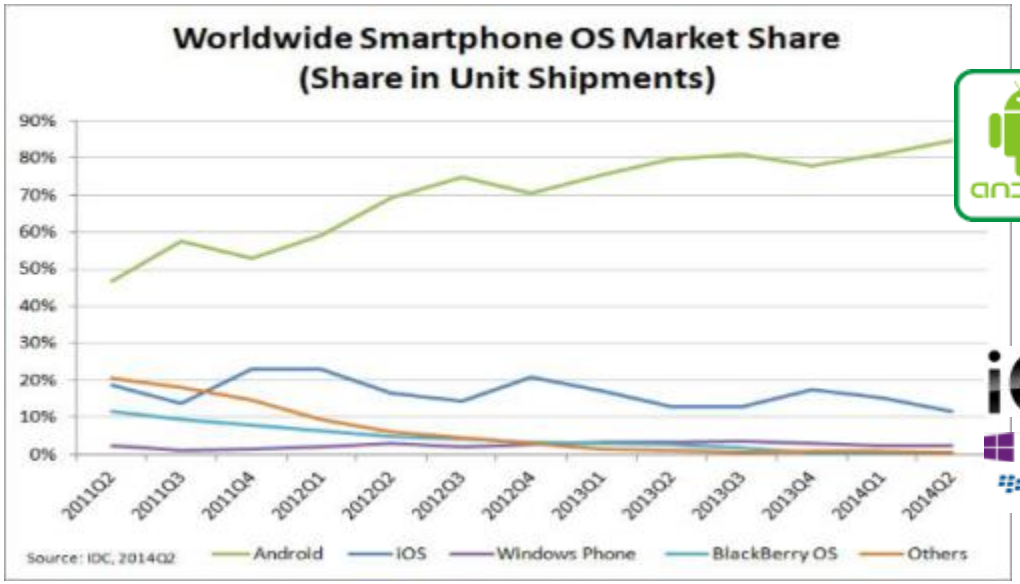
1. Teoría.
2. Práctica:
   a. Ejercicios prácticos a lo largo de la presentación.
   b. Práctica final Análisis de malware.

Índice

Introducción

¿Qué es Android? (I)

- Android es un sistema operativo para móviles desarrollado por la Open Handset Alliance lanzado en septiembre de 2008.
  - Sistema operativo open source basado en **Linux**.
  - En el segundo trimestre de 2014, se vendieron unos 255 millones de teléfonos Android, aglutinando un 85% de la masa de "smartphones" vendida:



Introducción

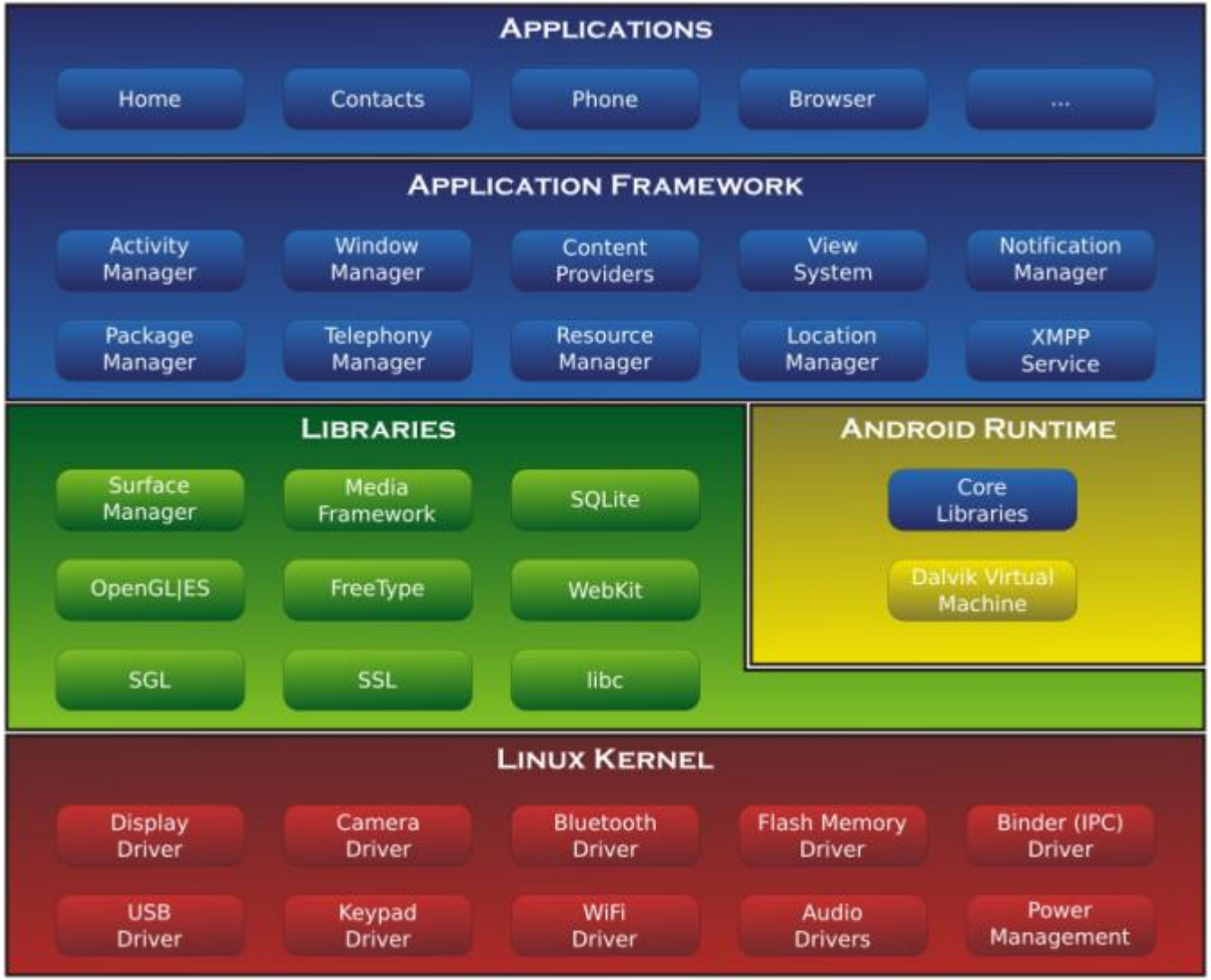
¿Qué es Android? (II)

- Características principales
  - Telefonía GSM
  - Bluetooth, EDGE, 3G/4G, WiFi, NFC
  - Pantalla táctil
  - Soporte para audio/vídeo/imágenes
  - Cámaras, GPS, brújula y acelerómetros
  - Soporte para aplicaciones desarrolladas por terceros: Marketplace de aplicaciones (Google Play)
    - En Julio de 2013 se sobrepasa el millón de aplicaciones disponibles.

Índice

Aplicaciones

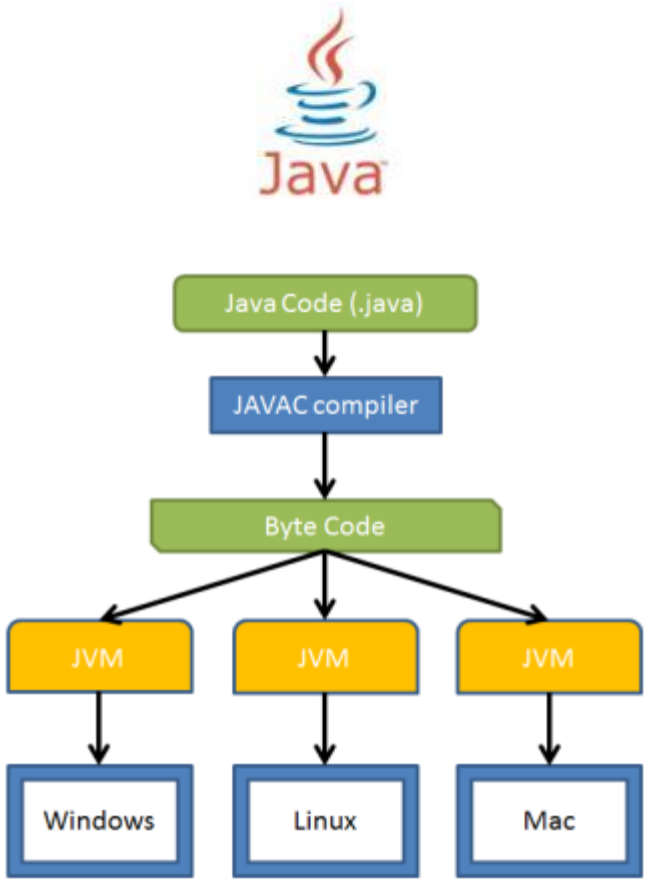
Arquitectura



Aplicaciones

JAVA

- Java es un lenguaje de programación orientado a objetos escrito por James Gosling y Sun Microsystems.
  - El nombre viene del tipo de café que se vendía en una cafetería cercana.
  - Actualmente es propiedad de Oracle.
  - Su principal fuerza es su portabilidad (WORA, "write once, run anywhere“).
  - Los programas son escritos en Java (ficheros .java) y compilados a “Java bytecode” (ficheros .class).
  - Requiere de una máquina virtual, la JVM (Java Virtual Machine), que ejecuta el Java bytecode.
  - 9 millones de desarrolladores.
  - El 89% de los ordenadores en EEUU ejecutan Java.



Aplicaciones

Práctica: crear una aplicación java (I)

- Programa Java que escribe 100 números aleatorios en un fichero

WriteToFile.java

```
1  // Programa que escribe 100 números aleatorios en un fichero
2  import java.io.PrintStream;
3  import java.io.IOException;
4  import java.io.File;
5  import java.util.Random;
6  public class WriteToFile {
7    public static void main(String[] args) {
8      try {
9      PrintStream writer = new PrintStream( new File("randInts.txt"));
10   Random r = new Random();
11   final int LIMIT = 100;
12   for(int i = 0; i < LIMIT; i++) {
13     writer.println( r.nextInt() );
14   }
15   writer.close();
16   }
17   catch(IOException e) {
18   System.out.println("An error occured");
19   }
20   }
21 }
22
```

line: 22 / 22 col: 0 sel: 0 INS TAB mode: Unix (LF) encoding: UTF-8 filetype: Java ...

Aplicaciones

Práctica: crear una aplicación java (II)

- 1: compilar el programa

```
Terminal
>> javac WriteToFile.java
```

- 2: ejecutar el programa

```
Terminal
>> Java WriteToFile
```

- 3: comprobación de la salida

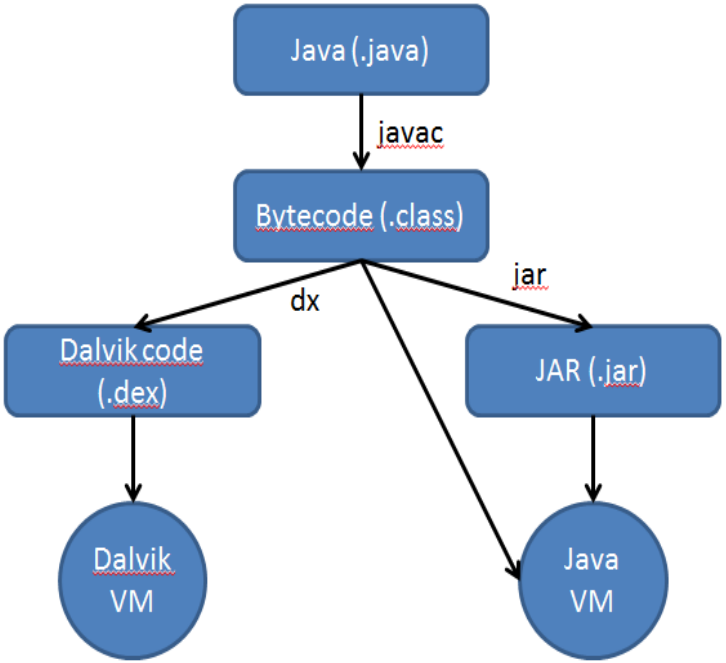
```
Terminal
>> cat randInts.txt
```

```
root@KALIGAB: ~/Desktop/android
File  Edit  View  Search  Terminal  Help
root@KALIGAB:~/Desktop/android#
root@KALIGAB:~/Desktop/android#
root@KALIGAB:~/Desktop/android# ls
WriteToFile.java
root@KALIGAB:~/Desktop/android# javac WriteToFile.java
root@KALIGAB:~/Desktop/android# ls
WriteToFile.class  WriteToFile.java
root@KALIGAB:~/Desktop/android# java WriteToFile
root@KALIGAB:~/Desktop/android# ls
randInts.txt  WriteToFile.class  WriteToFile.java
root@KALIGAB:~/Desktop/android# cat randInts.txt
721126882
2068912488
1174015008
1605108424
-676820507
-850056284
-2117216297
-2106062715
709215609
-1402807186
-1666748011
-309381205
1223680481
-1889372531
969043893
```

Aplicaciones

Dalvik

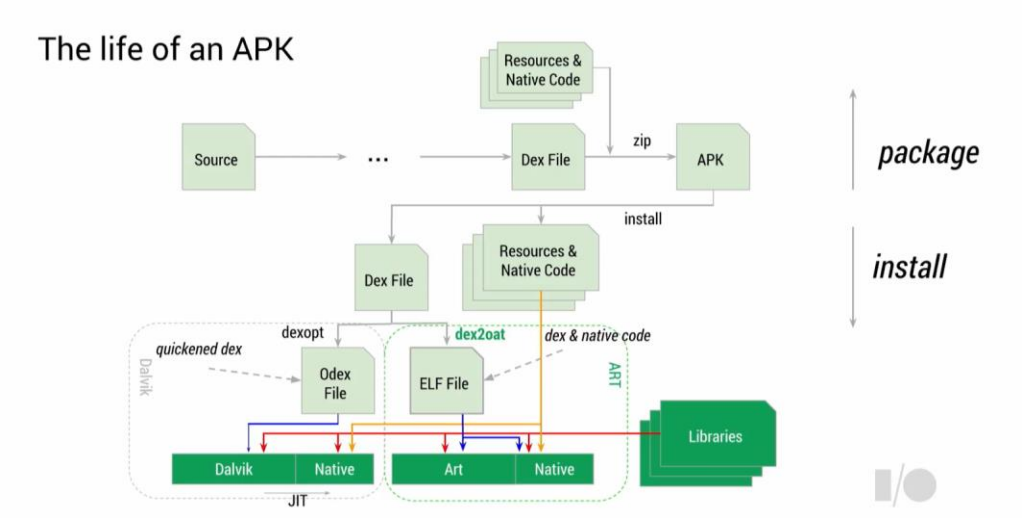
- "Máquina virtual" Java optimizada para Android
  - Escrito originalmente por Dan Bornstein. El nombre "Dalvik" viene de un pueblo pesquero en Eyjafjörður, Islandia.
  - Utiliza "Dalvik code" (ficheros .dex) en vez de ficheros .jar. Se pierde por lo tanto la portabilidad de Java.
  - Optimizado para ahorrar memoria y energía.
  - En proceso de sustitución por ART. Android 4.4 "KitKat" ya ofrece la posibilidad de ejecutar en ART.



Aplicaciones

ART

- Entorno de ejecución de aplicaciones en Android
- Disponible a partir de Android 4.4 KitKat
- Optimizado para ahorrar energía
- Inconvenientes:
  - Instalación más lenta de aplicaciones en el móvil
  - Necesidad de mayor espacio de almacenamiento para cada aplicación (20%)

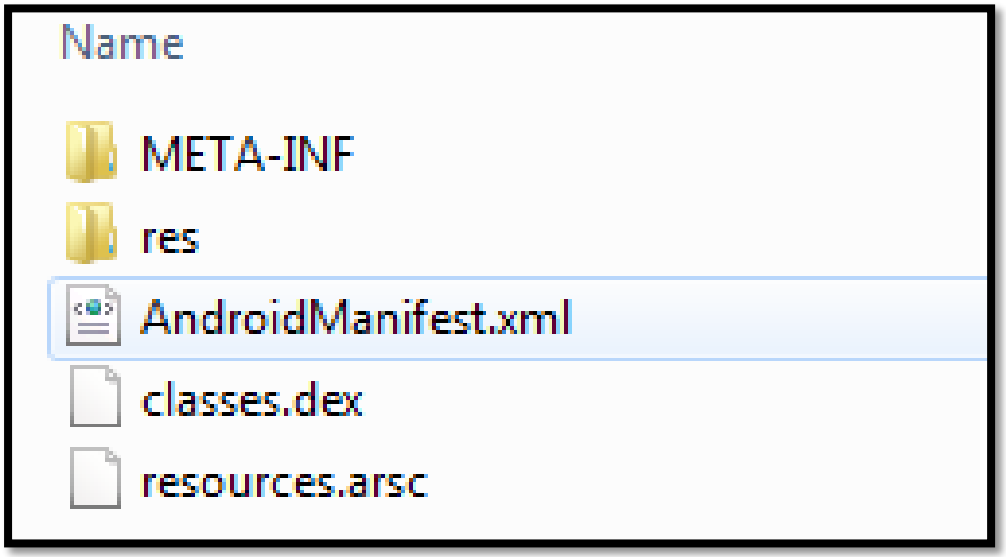


Comparativa entre las arquitecturas Dalvik y ART
http://www.elandroidelibre.com/2014/08/entendiendo-el-impacto-de-art-la-nueva-maquina-virtual-de-android.html

Aplicaciones

Paquetes APK

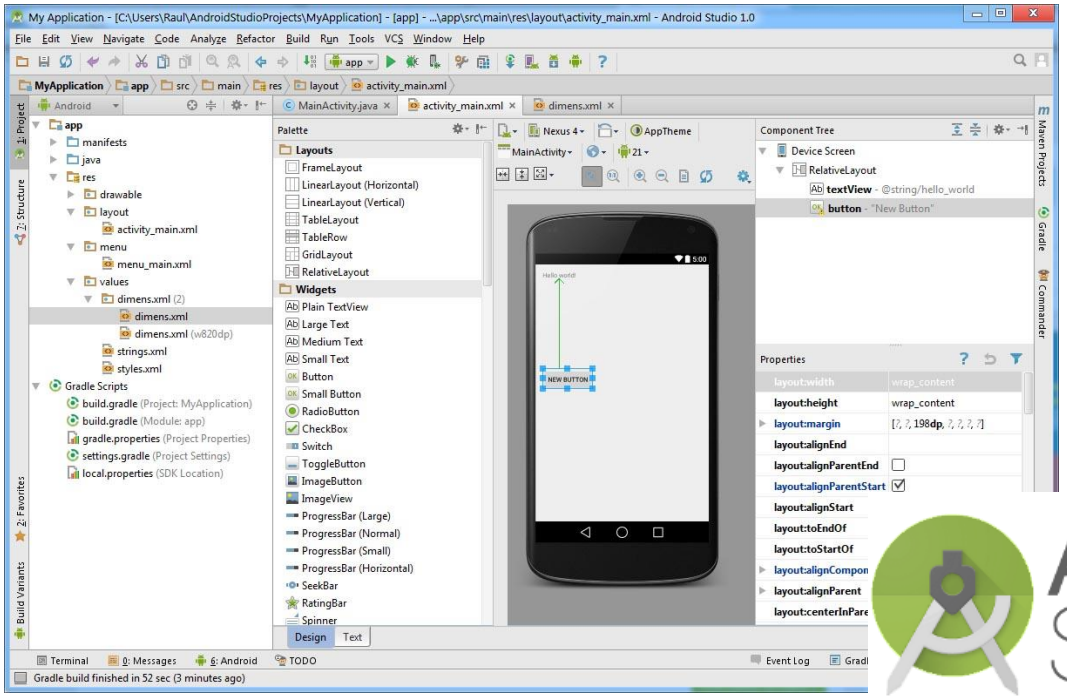
- Aplicación Android = fichero APK (**A**pplication **P**acKage **F**ile)
  - Un fichero APK es un **fichero zip** que contiene todos los recursos de una aplicación (ficheros .dex, imágenes, sonidos, etc.).
  - Una aplicación Android se ejecuta en su propia máquina virtual. Una aplicación sólo tiene acceso a sus recursos y sus datos (**sandbox**).
  - Un fichero APK contiene:
    - res
    - META-INF
    - ressources.arsc
    - **AndroidManifest.xml**
    - classes.dex
    - Otros



Aplicaciones

Práctica: aplicación Android (I)

- Las aplicaciones Android se suelen desarrollar en algún Entorno de Desarrollo Integrado (IDE, por sus siglas en inglés, *Integrated Development Environment*) como Eclipse, un programa de desarrollo libre.
- Iniciar Android Studio y abrir el proyecto “hello”.



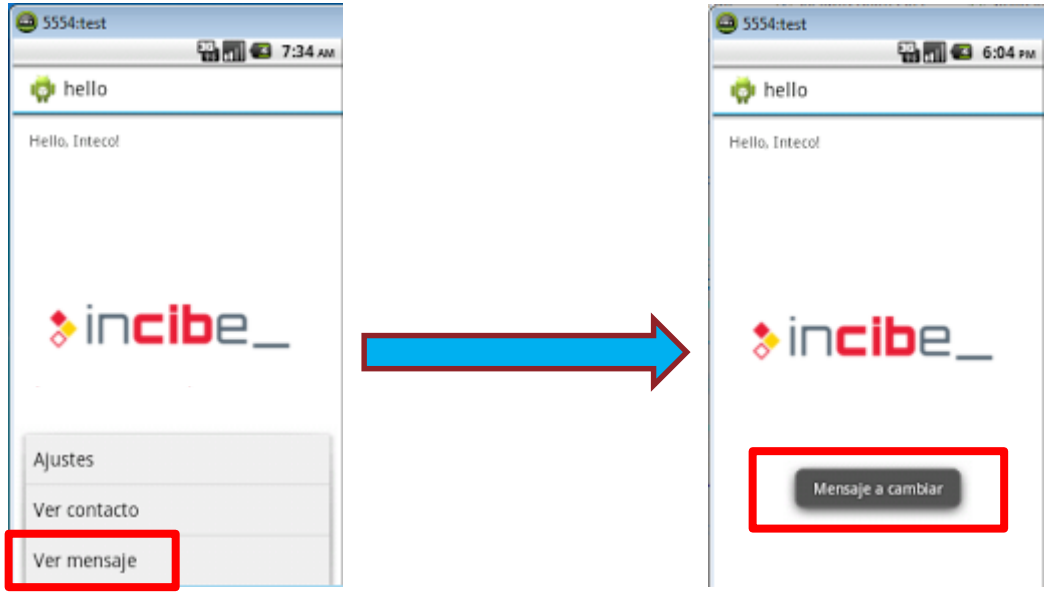
Android Studio

- Ejecutar el proyecto

Aplicaciones

Práctica: aplicación Android (IV)

- En la aplicación aparece el mensaje “Mensaje a cambiar”.
- **Reto**: ¿Podrías localizar el mensaje en el código fuente, cambiarlo y volver a ejecutar la aplicación para ver el cambio?



Aplicaciones

Google Play (I)

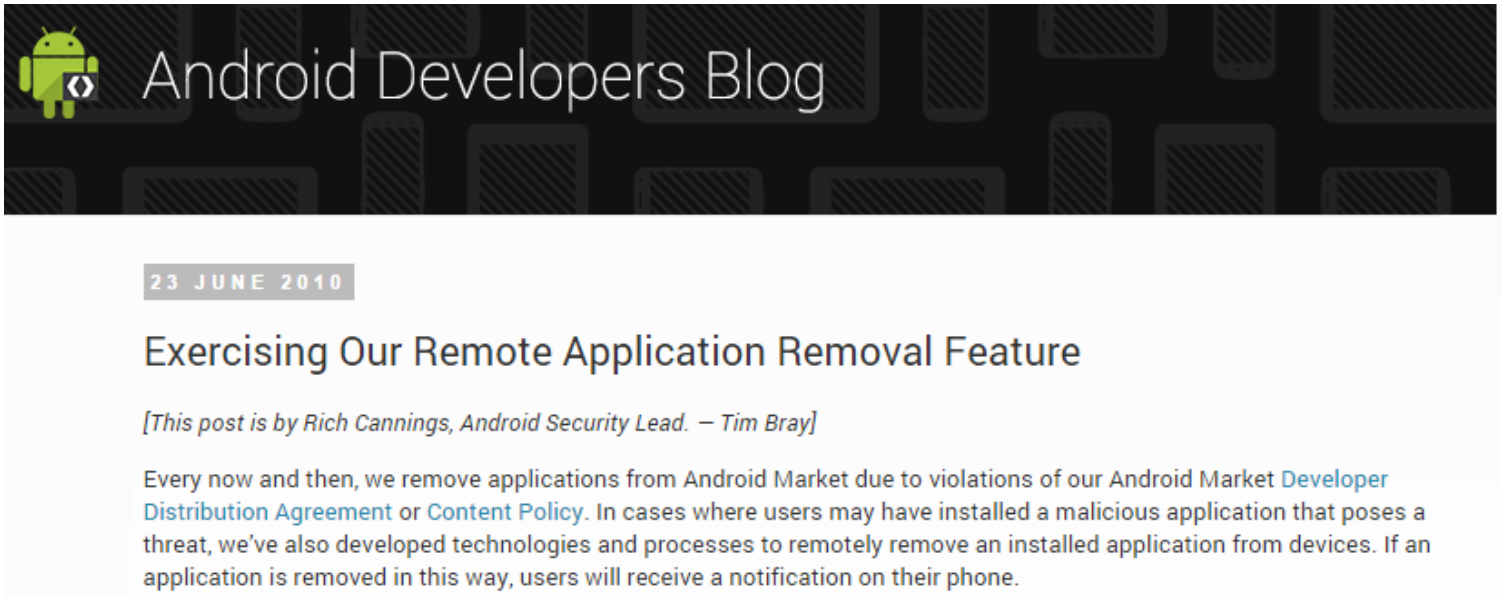
- Anteriormente **Android Market**.
- Permite acceder a **más de un millón** de aplicaciones.
- Controlado por Google: las aplicaciones contenidas en él son revisadas por la compañía aunque no el 100% son fiables (puesto que es una revisión automática).
- En el propio market existen aplicaciones malware
- **IMPORTANTE** revisar los permisos que se les da a las aplicaciones.

Google play

Aplicaciones

Google Play (II)

- Google conoce exactamente qué aplicaciones ha instalado un usuario.
- Google tiene la capacidad de **detectar** y **eliminar** aplicaciones maliciosas **remotamente** para proteger a los usuarios de todos los teléfonos Android.
- El borrado remoto de aplicaciones maliciosas por parte de Google evidencia que los controles efectuados sobre las aplicaciones publicadas en Google Play **no siempre son suficientes**.



Fuente: *http://android-developers.blogspot.com.es/2010/06/exercising-our-remote-application.html*

Aplicaciones

Google Play (III)

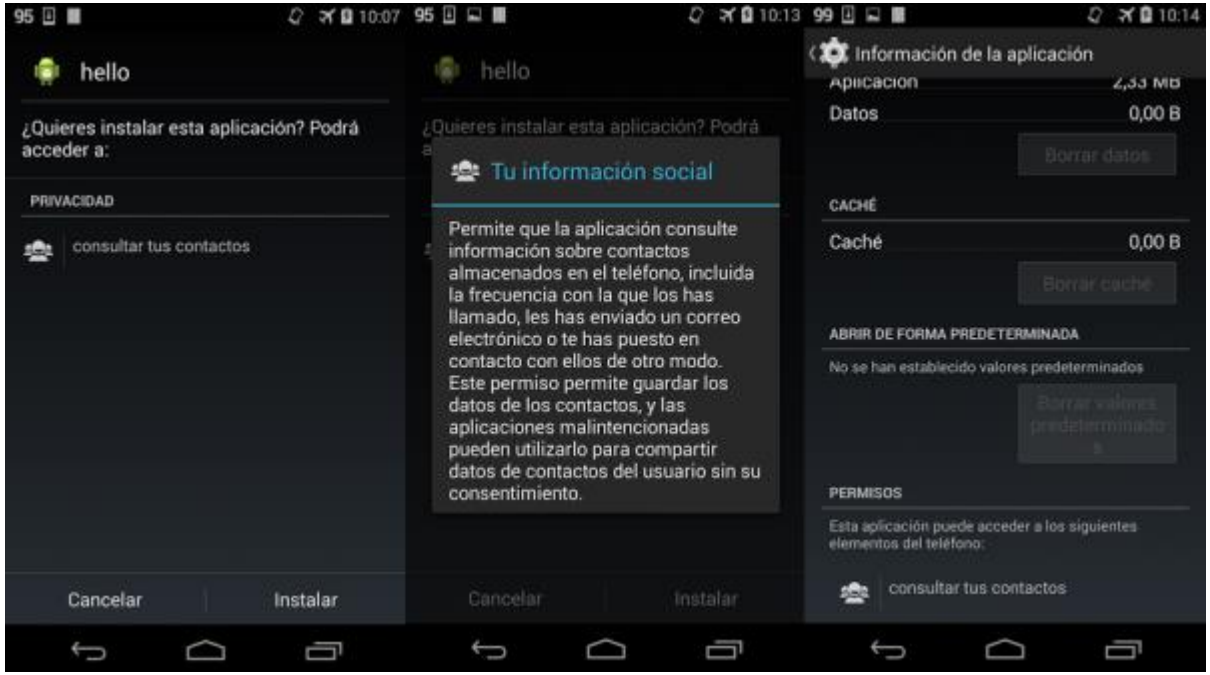
- Es posible instalar aplicaciones sin pasar por el Google Play activando los orígenes desconocidos:

Índice

Seguridad en Android

Sistema de permisos (I)

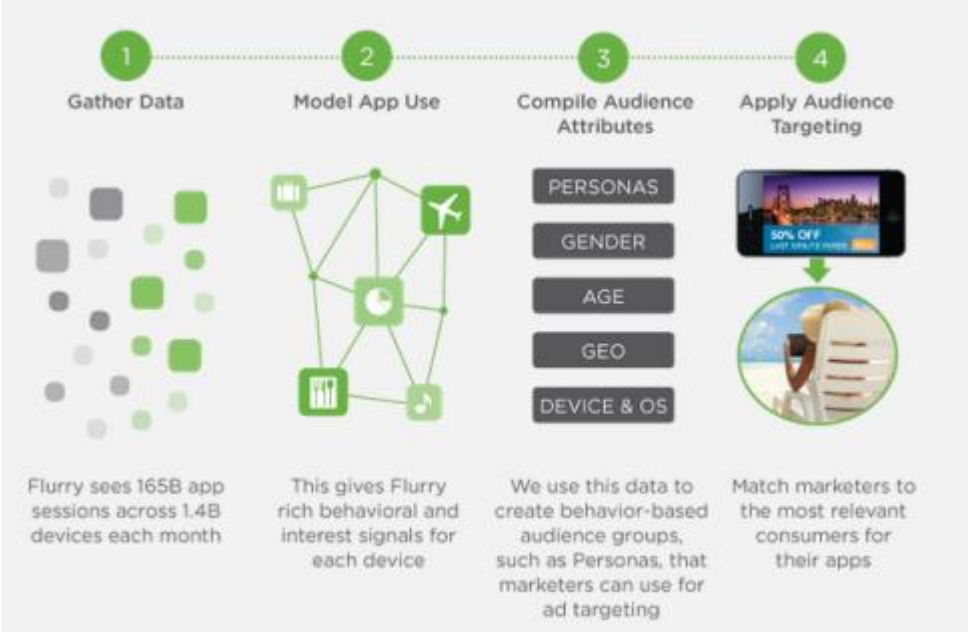
- Android utiliza un sistema de **permisos de aplicaciones** para proteger al usuario.
  - Dependiendo de la funcionalidad de la aplicación, requerirá de unos permisos concretos.
  - Por ejemplo, para utilizar la cámara, una aplicación necesita el permiso **android.permission.CAMERA**. Este permiso permite a la aplicación utilizar la cámara **incluso sin el consentimiento y sin interacción por parte del usuario** (una vez que el usuario lo autoriza al instalar la aplicación que solicita el permiso).



Seguridad en Android

Sistema de permisos (II)

- La necesidad de permisos excesivos puede deberse a varios motivos. Entre ellos, el más común es el acceso a datos personales para personalizar la publicidad.
  - Ejemplo: **Flurry**
    Flurry permite a los desarrolladores monetizar sus aplicaciones mediante publicidad personalizada.



Fuente: *http://www.flurry.com/solutions/advertisers/brands*

Seguridad en Android

Sistema de permisos (III): Androidmanifest.xml

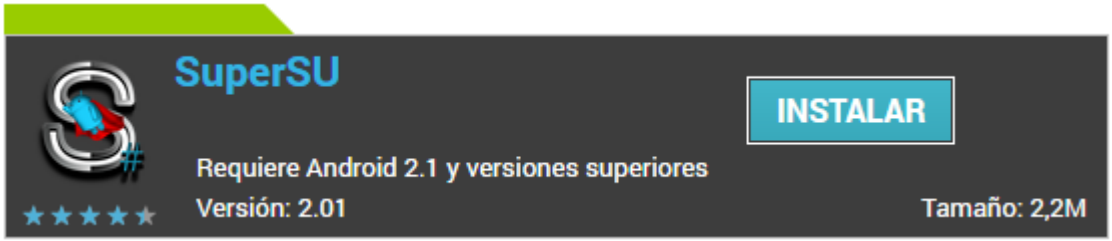
- Los permisos de las aplicaciones vienen definidos en el fichero AndroidManifest.xml, en las líneas “uses-permission”.
- La aplicación probada en el ejercicio 2 utiliza el permiso “READ_CONTACTS”:

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.hello"
    android:versionCode="1"
    android:versionName="1.0" >

    <uses-sdk
        android:minSdkVersion="8"
        android:targetSdkVersion="21" />
    <uses-permission android:name="android.permission.READ_CONTACTS"/>

    <application
        android:allowBackup="true"
        android:icon="@drawable/ic_launcher"
```

Seguridad en Android

Rooting

- En sistemas Unix, el usuario con máximos privilegios es **root** (raíz).
- Por defecto, Android no habilita esta característica para proteger al usuario.
- Es relativamente sencillo obtener permisos root en el teléfono. Se dice que se **rootea** el dispositivo, accediendo así a funciones muy avanzadas no orientadas al usuario final.
- Un teléfono rooteado es más potente, pero conlleva riesgos de seguridad. Una aplicación con permisos de root puede, por ejemplo, romper el ***sandboxing*** y acceder a datos de otras aplicaciones.
- Algunas aplicaciones como SuperSu mitigan parcialmente el riesgo de asignación de permisos root, concediendo estos permisos solamente a aplicaciones concretas.

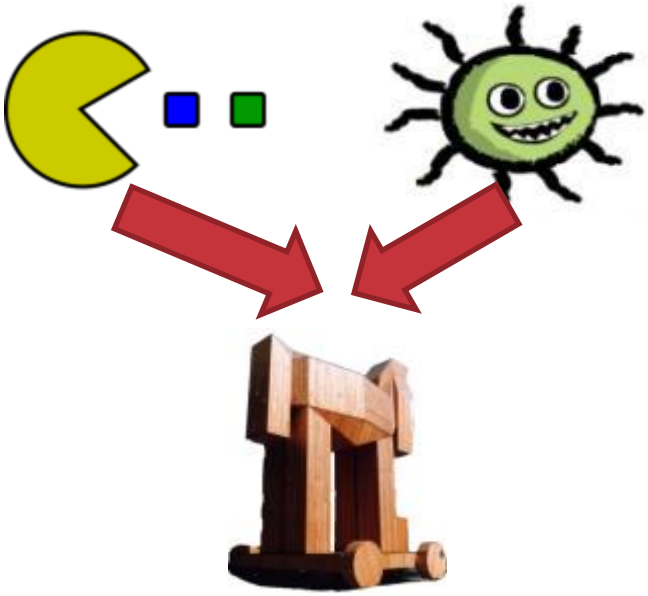


Índice

Malware

Malware: troyanos

- Un **troyano** o caballo de Troya es un **programa malicioso** (malware) que se presenta al usuario como un programa **aparentemente inofensivo**.
- El término proviene de la Odisea de Homero.
- Representan alrededor del 90% del software malicioso.



Programa + malware = troyano

Malware

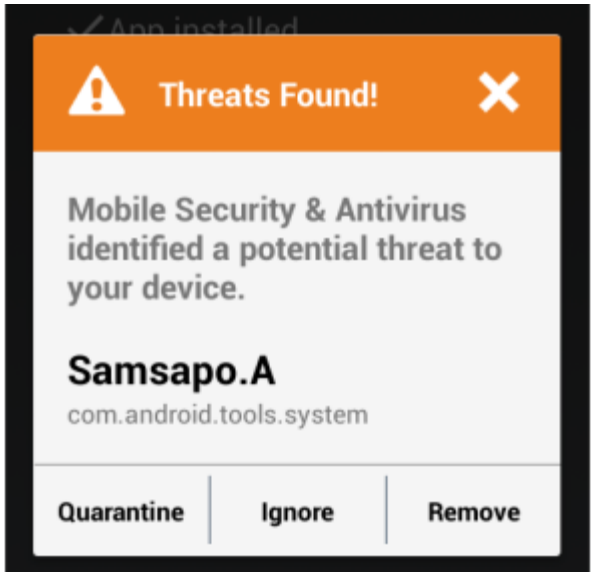
Malware: Gusanos (worms)

- Los gusanos (habitualmente llamados worms) son **programas maliciosos** que se propagan por la red de forma automática.
- Este tipo de malware es habitual en teléfonos, ya que este tipo de dispositivo conectado es idóneo para una propagación rápida (también muy comunes en PCs).
- El gusano más famoso, **Stuxnet**, es un malware supuestamente desarrollado por Israel y Estados Unidos diseñado para infectar **infraestructuras críticas** que infectó a 60.000 equipos en Irán.

Malware

Ejemplo: Samsapo (I)

- **Samsapo** es un gusano informático con aspecto de troyano que se propaga entre teléfonos Android.
- Envía de forma automática a todos los contactos del teléfono un SMS para propagarse.
- El mensaje de texto incluye la frase "¿Ésta es tu foto?" y un enlace para descargarse el APK malicioso. Este tipo de engaño al usuario es característico del malware (Ingeniería Social).
- Una vez instalado el APK, éste vuelve a propagarse y realiza acciones maliciosas como robo de datos, envío de mensajes de alto coste (premium), etc.



Fuente: http://www.welivesecurity.com/2014/04/30/android-sms-malware-catches-unwary-users/

Malware

Ejemplo: Samsapo (II)

- Los permisos solicitados por Samsapo son los siguientes (contenido del **AndroidManifest.xml**):

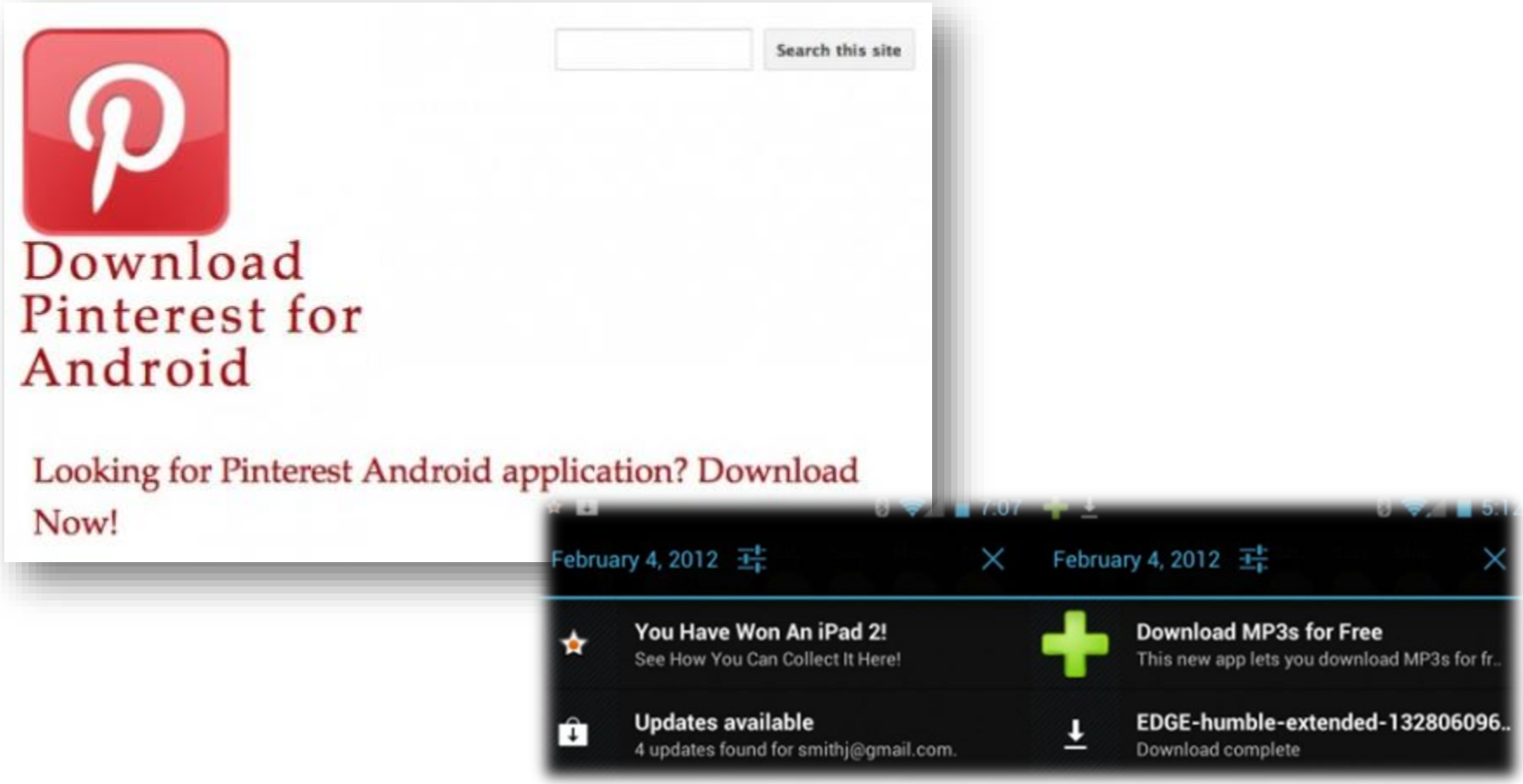
```
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.WRITE_SMS" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.MODIFY_PHONE_STATE" />
<uses-permission android:name="android.permission.CALL_PHONE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.READ_CALL_LOG" />
<uses-permission android:name="android.permission.WRITE_CALL_LOG" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.INSTALL_PACKAGES" />
<uses-permission android:name="android.permission.DELETE_PACKAGES" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
```

- Una buena forma de identificar un malware es fijándose en los permisos que requiere y analizando si éstos son necesarios para la funcionalidad de la aplicación. Por ejemplo, una aplicación de linterna que requiera permisos para hacer llamadas es un buen candidato a troyano.

Malware

Ejemplo: falso pinterest

- Un Pinterest falso se publicó en el Android Market. En realidad se trataba de un malware que bombardeaba al usuario con publicidad engañosa:



Fuente: *http://www.gottabemobile.com/2012/02/05/pinterest-for-android-pins-spam-to-your-notification-bar/*

Índice

Vulnerabilidades

Vulnerabilidades en Android

- Los ejemplos anteriores no utilizan vulnerabilidades del sistema sino que manipulan al usuario (troyanos).
- Como en cualquier programa informático, en Android existen vulnerabilidades que, si se explotan correctamente, permiten realizar ataques más complejos y avanzados.
- Muchas de esas vulnerabilidades son públicas y pueden ser consultadas:

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score
1	CVE-2011-2344	310		+Priv	2011-07-08	2011-07-08	10.0
Android Picasa in Android 3.0 and 2.x through 2.3.4 uses a cleartext HTTP session when transmitting the au access private pictures and web albums by sniffing the token from connections with picasaweb.google.com.							
2	CVE-2010-1807	20		DoS Exec Code	2010-09-10	2012-09-14	9.3
WebKit in Apple Safari 4.x before 4.1.2 and 5.x before 5.0.2; Android before 2.2; and webkitgtk before 1.2 arbitrary code or cause a denial of service (application crash) via a crafted HTML document, related to non-							
3	CVE-2011-3874	119		Exec Code Overflow	2012-01-27	2012-02-06	9.3
Stack-based buffer overflow in libsysutils in Android 2.2.x through 2.2.2 and 2.3.x through 2.3.6 allows use FrameworkListener::dispatchCommand method with the wrong number of arguments, as demonstrated by							
4	CVE-2011-3918	399		DoS	2012-10-07	2012-10-08	7.8
The Zygote process in Android 4.0.3 and earlier accepts fork requests from processes with arbitrary UIDs, application.							
5	CVE-2012-4220			DoS Exec Code	2012-11-30	2012-12-18	7.5
diagchar_core.c in the Qualcomm Innovation Center (QuIC) Diagnostics (aka DIAG) kernel-mode driver fo service (incorrect pointer dereference) via an application that uses crafted arguments in a local diagchar_ic							

Fuente: *http://www.cvedetails.com/*

Vulnerabilidades

Explotación de vulnerabilidad: adobe reader vulnerable

- Una versión obsoleta de Adobe Reader para Android permitía ejecutar código malicioso en el teléfono utilizado archivos PDF con código embebido:

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-0514	264		Exec Code	2014-04-15	2014-04-24	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

The Adobe Reader Mobile application before 11.2 for Android does not properly restrict use of JavaScript, which allows remote attackers to execute arbitrary code via a crafted PDF document, a related issue to CVE-2012-6636.

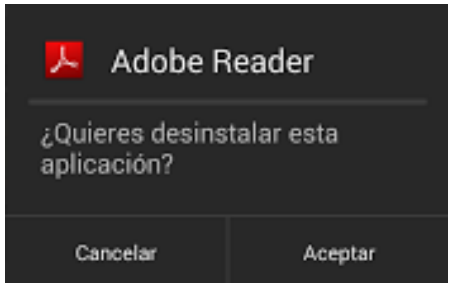
- Todos los teléfonos Android con una versión de Adobe Reader anterior a 11.2 pueden ser comprometidos si abren un archivo PDF malicioso.

Fuente: *http://www.cvedetails.com/*

Vulnerabilidades

Práctica: Explotación de vulnerabilidad

- 1) Desinstalar la actual versión de Adobe Reader.
- 2) Instalar la versión de Adobe Reader vulnerable.
- 3) Abrir el archivo “malo.pdf” y pulsar el botón “Click me”.



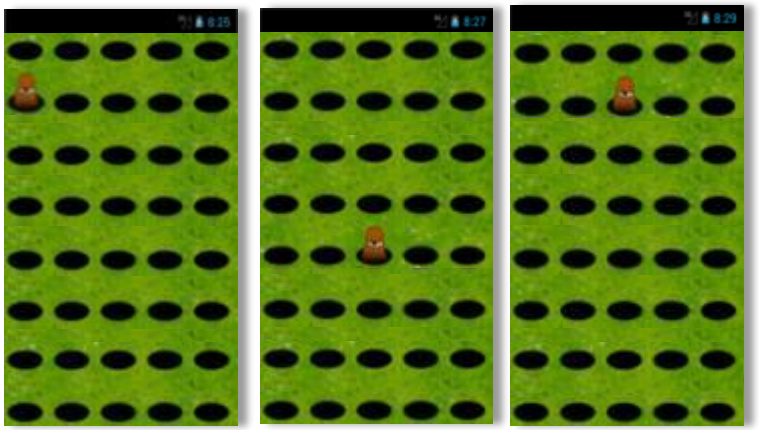
NOTA: el PDF sólo crea un archivo de texto y no realiza acciones maliciosas.

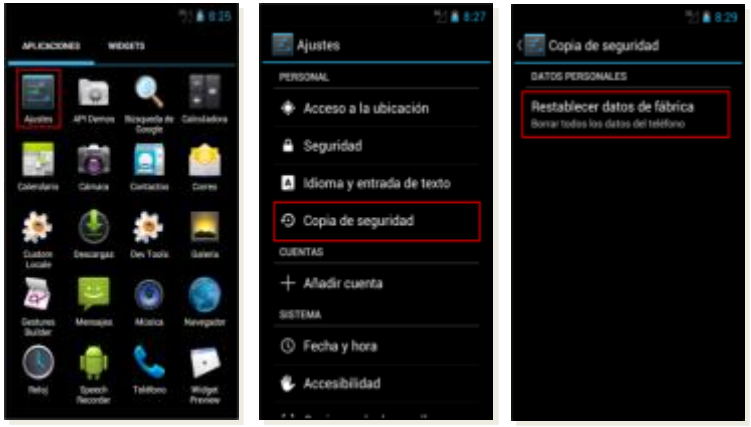
Vulnerabilidades

Explotación de vulnerabilidad: tapjacking (I)

- El tapjacking es una vulnerabilidad presente en dispositivos Android anteriores a 4.0.
- Permite utilizar las notificaciones “toast” para simular falsos botones que ocultan botones reales.

Lo que el usuario ve





Lo que realmente está pasando

Vulnerabilidades

Explotación de vulnerabilidad: tapjacking (II)

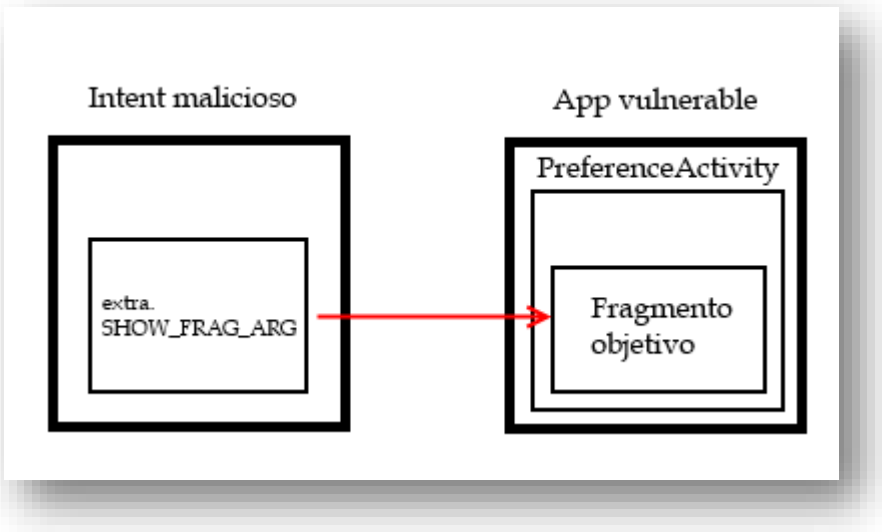
Ejemplo de tapjacking:

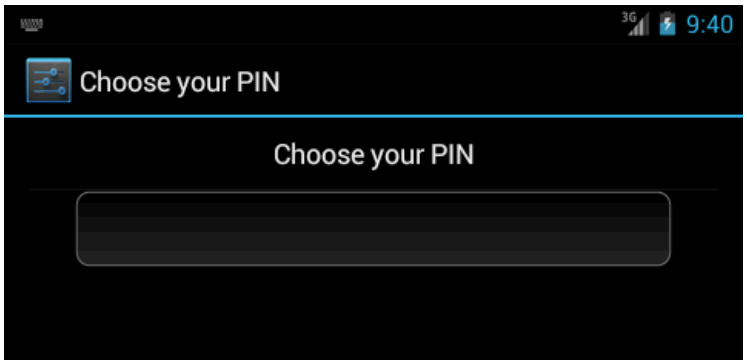
https://www.youtube.com/watch?v=gCLU7YUXUAY

Vulnerabilidades

Explotación de vulnerabilidad: fragment injection

- Vulnerabilidad presente en todos los teléfonos Android anteriores a Kitkat, permite manipular aplicaciones legítimas desde otra maliciosa.
- Funciona llamando a la aplicación legítima con un “intent” y una opción especial que permite invocar a un fragmento de la aplicación legítima que no debería ser accesible desde otras aplicaciones.





Este fragmento permite cambiar el pin del móvil. Se ha accedido sin tener que poner el pin anterior gracias a la inyección.

Índice

Contramedidas

¿Cómo me protejo del malware en Android? (I)

- La regla de oro: **sentido común**

Fuente: *http://tecnosimple.com/descargar-escaner-para-desnudar-gratis-para-celular/*

Contramedidas

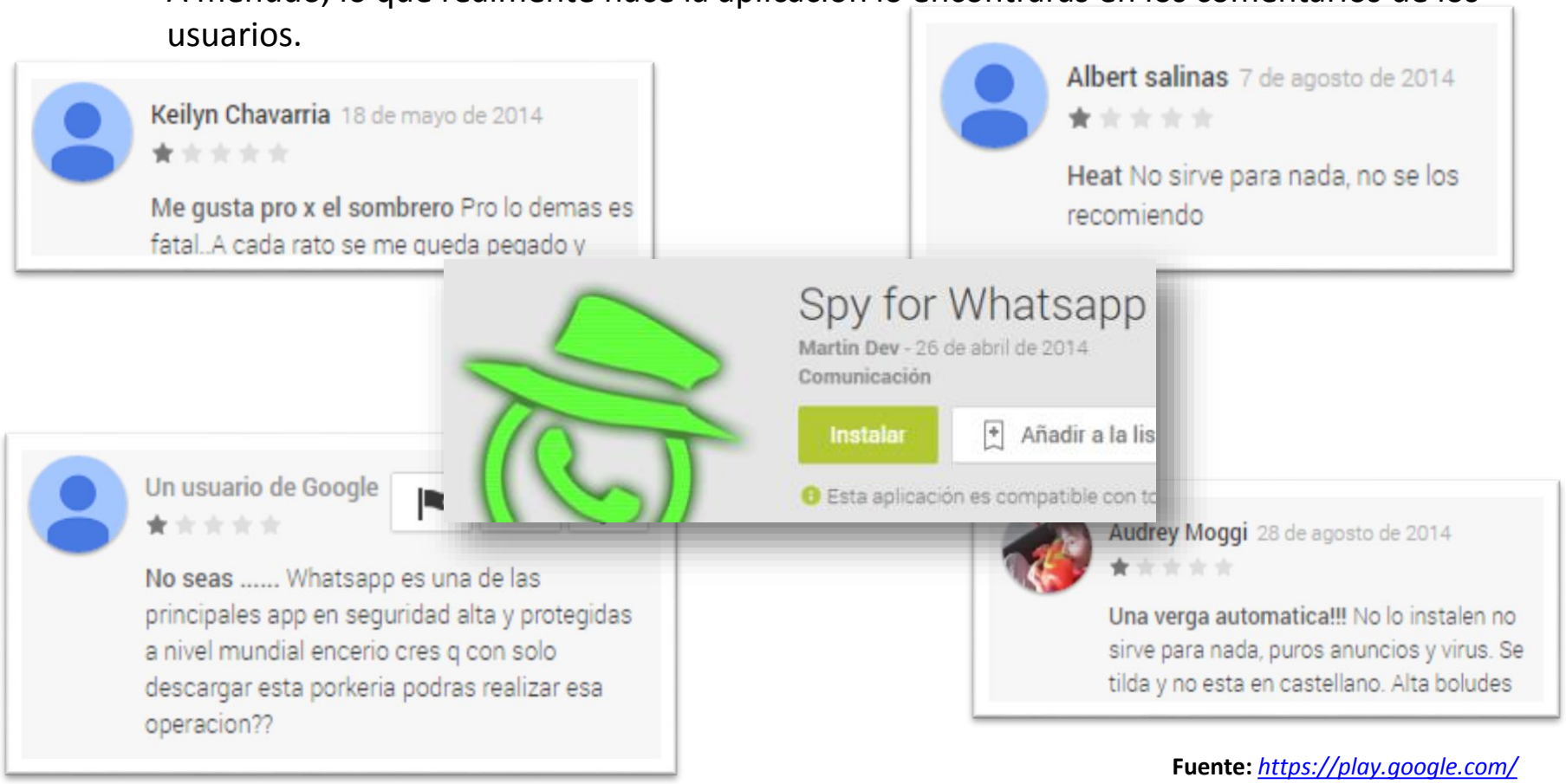
¿Cómo me protejo del malware en Android? (II)

- No descargues aplicaciones pirata y/o de origen desconocido
  - Se ha comprobado que muchos troyanos se esconden en aplicaciones pirateadas. A veces es mejor gastarse 1 euro que correr un riesgo de infección. En general, no es recomendable habilitar la instalación de aplicaciones de origen desconocido.
    Sé especialmente cuidadoso con las aplicaciones que requieren permisos de root.
- Examina los permisos requeridos por la aplicación
  - Examinando los permisos podrás saber a priori a qué podrá acceder la aplicación.
- Comprueba el desarrollador
  - Si el desarrollador no es conocido, busca en Google para asegurarte que es de confianza. Desarrolladores como “Kingmall2010” o “we20090202” deberían levantar sospechas.
- Instala un antivirus
  - Android también tiene antivirus.

Contramedidas

¿Cómo me protejo del malware en Android? (III)

- Consulta las valoraciones y puntuaciones
  - A menudo, lo que realmente hace la aplicación lo encontrarás en los comentarios de los usuarios.



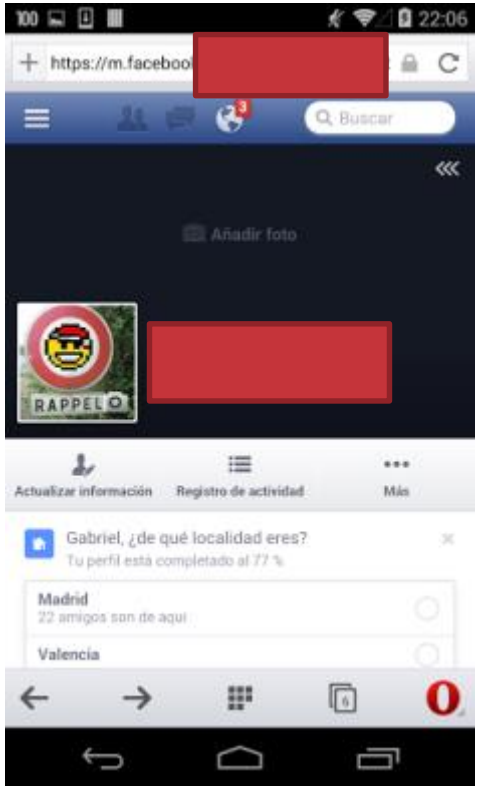
Fuente: *https://play.google.com/*

Índice

Práctica: analizando un malware

Analizando un malware

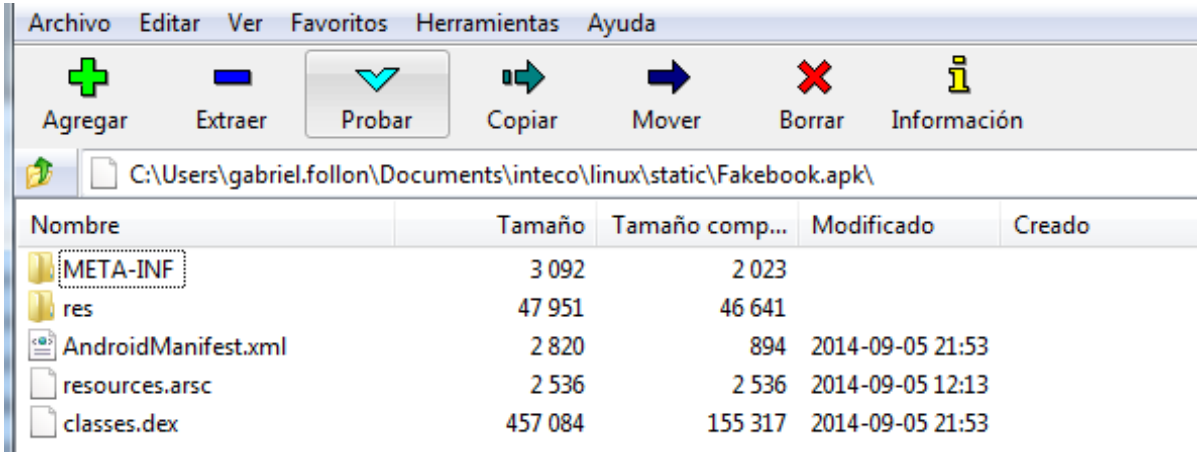
- Aplicación falsa de “Fakebook” que roba datos privados de la víctima, enviándolos a un servidor controlado por el atacante.
- Es un troyano: se hace pasar por una aplicación legítima.
- Mientras procesa los datos, redirige al usuario a la página de facebook legítima para no levantar sospechas.



Práctica: analizando un malware

Paso 1: descomprimir el apk

- El primer paso de nuestro análisis será descomprimir el apk con cualquier herramienta que maneje ficheros zip:



- El fichero AndroidManifest.xml no es directamente legible, ya que está en formato binario. La herramienta **apktool** permite transformar ese fichero a formato texto:

```
C:\Users\root\Desktop\static>java -jar apktool.jar d Fakebook.apk Facebook_data
I: Baksmaling...
I: Loading resource table...
I: Loaded.
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\root\apktool\framework\1.apk
I: Loaded.
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Done.
I: Copying assets and libs...

C:\Users\root\Desktop\static>
```

Práctica: analizando un malware

Paso 2: analizar el androidmanifest.xml

- Se observan permisos como READ_CONTACTS o READ_PHONE_STATE:

```
<?xml version="1.0" encoding="UTF-8"?>
- <manifest xmlns:android="http://schemas.android.com/apk/res/android"
  package="com.fakebook" android:versionName="1.0" android:versionCode="1">
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission
        android:name="android.permission.ACCESS_LOCATION_EXTRA_COMMANDS"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
  - <application android:allowBackup="true" android:debuggable="true"
    android:icon="@drawable/ic_launcher" android:label="@string/app_name"
    android:theme="@style/AppTheme">
      - <activity android:name="com.fakebook.MainActivity"
        android:label="@string/app_name">
          - <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

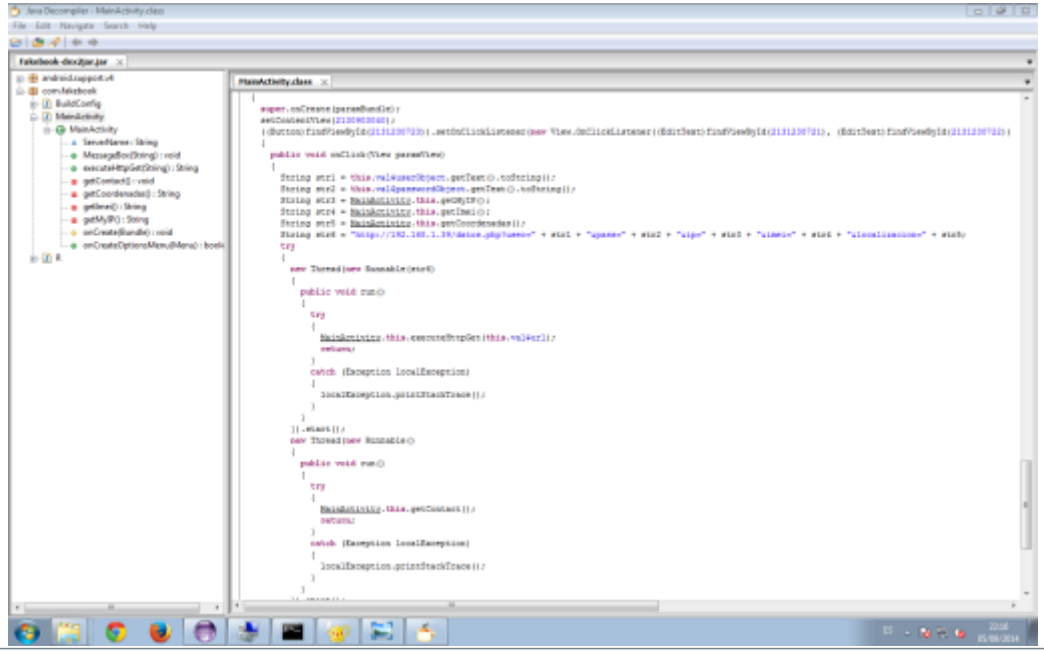
Práctica: analizando un malware

Paso 3: “decompilar” el programa y obtener el código fuente

- Utilizando **dex2jar**, se obtiene un equivalente **jar** a partir del fichero **dex** obtenido en el paso anterior:

```
C:\Users\root\Desktop\static\dex2jar-0.0.9.15>d2j-dex2jar.bat Fakebook.apk
dex2jar Fakebook.apk -> Fakebook-dex2jar.jar

C:\Users\root\Desktop\static\dex2jar-0.0.9.15>
```

- A partir del fichero **jar**, se obtiene el código fuente con la herramienta **Java Decompiler**:



Práctica: analizando un malware

Paso 4: análisis de código

- Una vez obtenido el código, se puede realizar una búsqueda estratégica para identificar rápidamente sentencias sospechosas:
  - Acceso a SQLITE: db, sqlite, database, insert, delete, select, table, cursor…
  - Notificaciones toast (tapjacking): toast
  - Identificadores: uid, user-id, imei, deviceId, deviceSerialNumber…
  - **Conexiones**: http, url, HttpURLConnection, URLConnection…
  - Intents
  - Localización GPS: getLastKnownLocation, requestLocationUpdates, getLatitude…

Índice

Resumen

Cuestiones

1. ¿Qué lenguaje de programación se utiliza para crear aplicaciones en Android? ¿Qué herramienta se utiliza para desarrollarlas?

2. ¿En qué basa Android la seguridad de sus aplicaciones?

3. ¿Qué significa “rootear” el teléfono? ¿Qué riesgos conlleva?

4. ¿De dónde suele proceder el malware en Android?

5. ¿Qué medidas se pueden tomar para protegerse?

Fuente: https://www.virustotal.com/es/

Resumen

Resumen de conceptos

1. JAVA es el lenguaje de programación para realizar aplicaciones en Android. Para crearlas se suele utilizar algún entorno de desarrollo integrado, IDE (por sus siglas en inglés), que son plataformas de programación, desarrollo y compilación; para las aplicaciones en Android se suele emplear Android Studio.

2. Android utiliza un sistema de permisos. Cada aplicación tiene un fichero "AndroidManifest.xml" donde se especifica los permisos que necesita la aplicación para ejecutarse y que debe aprobar el usuario para instalarla.

3. Cuando se rootea el dispositivo se accede a funciones avanzadas no orientadas al usuario final. Un teléfono rooteado es más potente, pero una aplicación con permisos de root puede romper el sandboxing y acceder a datos de otras aplicaciones.

4. Suele proceder de las aplicaciones. A veces de las descargadas de Google Play, aunque se suele corregir en cuanto se detecta, y otras veces de aplicaciones descargadas desde otras fuentes.

5. Google revisa de forma automática las aplicaciones contenidas en Google Play. Como usuarios nos podemos proteger revisando los permisos de las aplicaciones antes de instalarlas y teniendo instalado un antivirus en nuestro dispositivo.

Índice

Encuesta de satisfacción

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Encuesta satisfacción

Estimado alumno, te agradecemos que hayas asistido a esta Jornada y esperamos que te haya resultado interesante. Nos gustaría conocer tu opinión de cara a poder mejorar en las próximas Jornadas, por este motivo te pedimos que, por favor, rellenes esta encuesta.

La encuesta es totalmente anónima y no se recabará ningún dato personal tuyo

¡Muchas gracias por tu colaboración!

*Obligatorio

Nombre de la jornada *

Fecha y hora de la jornada *

Día | Mes | 2015 | h : min

Datos generales

Nombre de tu centro de estudios *

Actuaciones
I+D+i y Promoción de Talento en Ciberseguridad

Este taller y el resto de las Jornadas "Espacio de Ciberseguridad" forman parte del «**Eje V: Programa de Excelencia en Ciberseguridad**» dentro del **Plan de Confianza Digital** del Ministerio de Industria, Energía y Turismo (**MINETUR**) que se está llevando a cabo desde **INCIBE** para la **promoción y captación de talento en Ciberseguridad**.

Si te gusta la ciberseguridad y quieres profundizar en este tema, dentro del Plan de Confianza Digital se están desarrollando las siguientes actividades y eventos de ciberseguridad:

- **Formación especializada en ciberseguridad:** MOOC que se desarrollan a través de la plataforma de formación de INCIBE (http://formacion-online.incibe.es) sobre conceptos avanzados en ciberseguridad tales como ciberseguridad industrial, seguridad en dispositivos móviles, programación segura, malware y sistemas TI.

- **Programa de becas:** Programa de becas anual en el que se establecerán diferentes tipologías de becas: formación de cursos especializados y másteres en ciberseguridad, y becas de investigación. Todas las publicaciones de este tipo se realizará a través de la siguiente página https://www.incibe.es/convocatorias/ayudas/.

- **Evento de ciberseguridad – CyberCamp** (http://cybercamp.es).

CyberCamp es el evento internacional de INCIBE para identificar, atraer y promocionar el talento en ciberseguridad.

- Identificar trayectorias profesionales de los jóvenes talento.
- Detectar y promocionar el talento mediante talleres y retos técnicos.
- Atraer el talento ofreciendo conferencias y charlas de ciberseguridad por profesionales y expertos de primer nivel.

Y muchas cosas más….

- Evento para **familias**, contando con actividades de concienciación y difusión de la ciberseguridad para padres, educadores e hijos.
- Promoción de la **industria** e **investigación** en ciberseguridad.

https://cybercamp.es/

https://twitter.com/CybercampEs

https://www.facebook.com/CyberCampEs

Gracias

por tu atención

Contáctanos

Contacto (más información y dudas sobre las jornadas):

espaciosciberseguridad@incibe.es

En las redes sociales:

@incibe
@certsi
@osiseguridad
@CyberCampES

Oficina de Seguridad del internauta
(Pienso luego clico)

INCIBE
OSIseguridad

Oficina de Seguridad del internauta
CyberCamp

Pág. INCIBE
Grupo INCIBE

Oficina de Seguridad del internauta

En la sede:
Avenida José Aguado, 41 - Edificio INCIBE
24005 León
Tlf. 987 877 189

En los sitios web:
www.incibe.es
www.osi.es
www.cybercamp.es

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

NATIONAL CYBERSECURITY INSTITUTE OF SPAIN

incibe_

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO