

Tema 5. Detección de problemas de seguridad en aplicaciones para dispositivos móviles

Arquitectura de los sistemas Android e iOS.



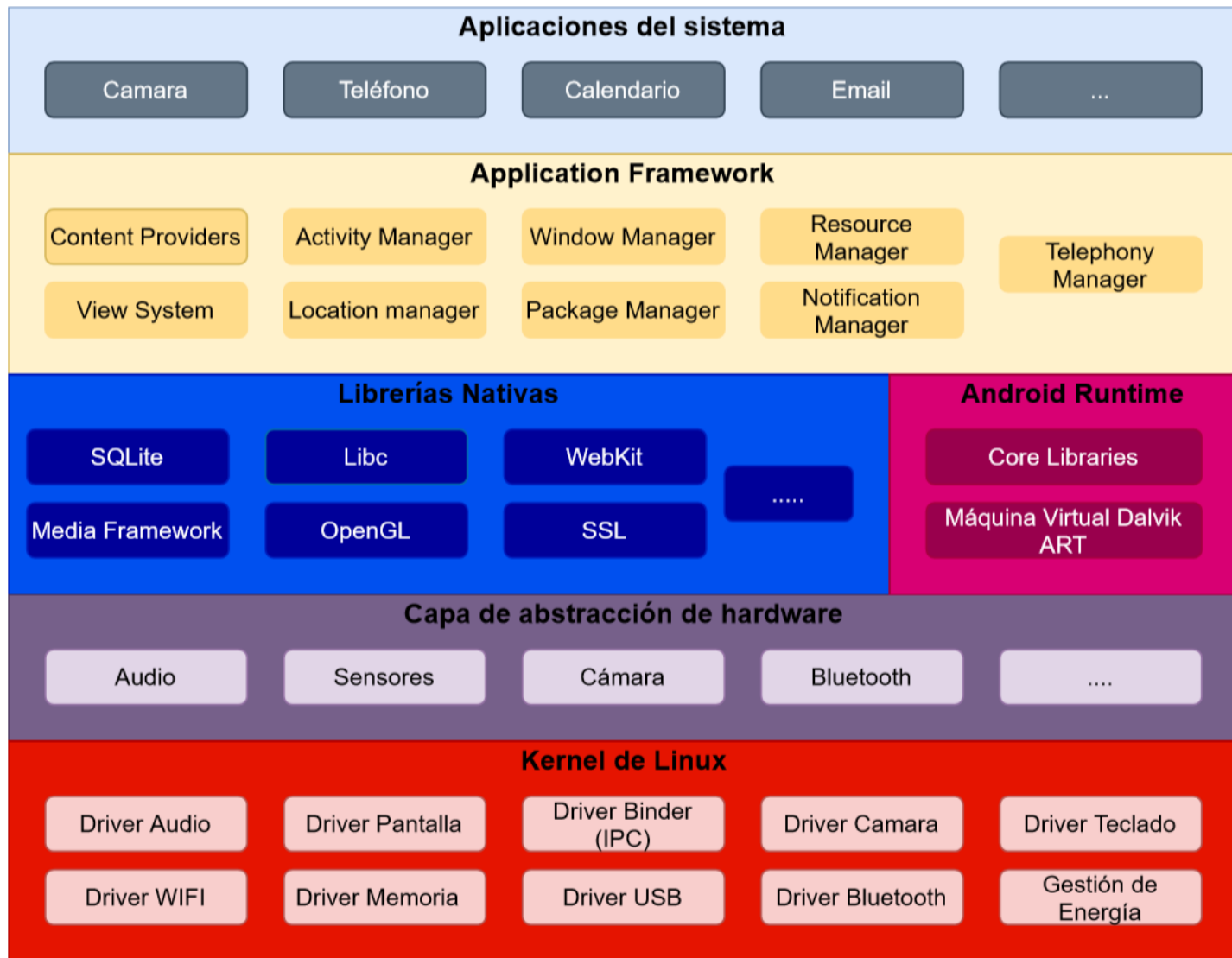
UNIÓN EUROPEA

Fondo Social Europeo
EL FSE invierte en tu futuro

Android

- Disponible para distintos tipos de arquitecturas → x86, x86_64, ARM...
- Basado en el kernel de Linux.
- Aplicaciones ejecutadas por el Android Runtime o ART (sucesor de Dalvik).
- Soporta varios sistemas de ficheros → EXT4, JFFS2, YAFFS2...
- Soporta cifrado de disco.
- Es open source, basado en una licencia Apache 2.0.

Arquitectura del sistema Android



Java API Framework

Android

- Proporciona acceso a los desarrolladores a distintas funcionalidades de la plataforma:
 - **Activity Manager:** se encarga de gestionar las distintas actividades que aparecen por pantalla. Gestiona el ciclo de vida de una actividad.
 - **Content Providers:** proporciona una interfaz para almacenar y acceder a los datos de las aplicaciones. Las aplicaciones pueden crear content providers y exponer sus datos a otras aplicaciones.
 - Ejemplo: acceso de WhatsApp a tus contactos.
 - **Notification Manager:** para gestionar y notificar al usuario los eventos que ocurren en las aplicaciones (información de la barra de estado y panel de notificaciones).
 - **Location Manager:** proporciona acceso a la información relacionada con la ubicación (mediante GPS, WIFI, etc).

Java API Framework

Android

- **View System:** se encarga de gestionar las diferentes vistas (interfaces de usuario) que presenta una aplicación.
 - Listas, cuadrículas, botones, menús desplegables, cuadros de texto...
- **Package Manager:** gestiona la información relacionada con los paquetes instalados en el sistema.
- **Telephony Manager:** gestiona la información relacionada con los servicios de telefonía.
 - Subscriber ID, SIM serial number, tipo de red móvil, roaming...
- Más información sobre librerías de Android:
<https://developer.android.com/reference/packages>

Particiones

Android

Particiones en Android



Tarjeta SD



Particiones

Android

- **Boot:** partición de arranque del sistema. Contiene el kernel.
- **System:** partición del sistema operativo. Contiene los archivos del SO y las aplicaciones del sistema que vienen preinstaladas.
- **Recovery:** partición de recuperación. Alternativa a la partición boot que permite al dispositivo iniciar en modo “recovery”.
- **Data:** partición que contiene los datos de usuario como las aplicaciones instaladas, contactos, mensajes, etc.

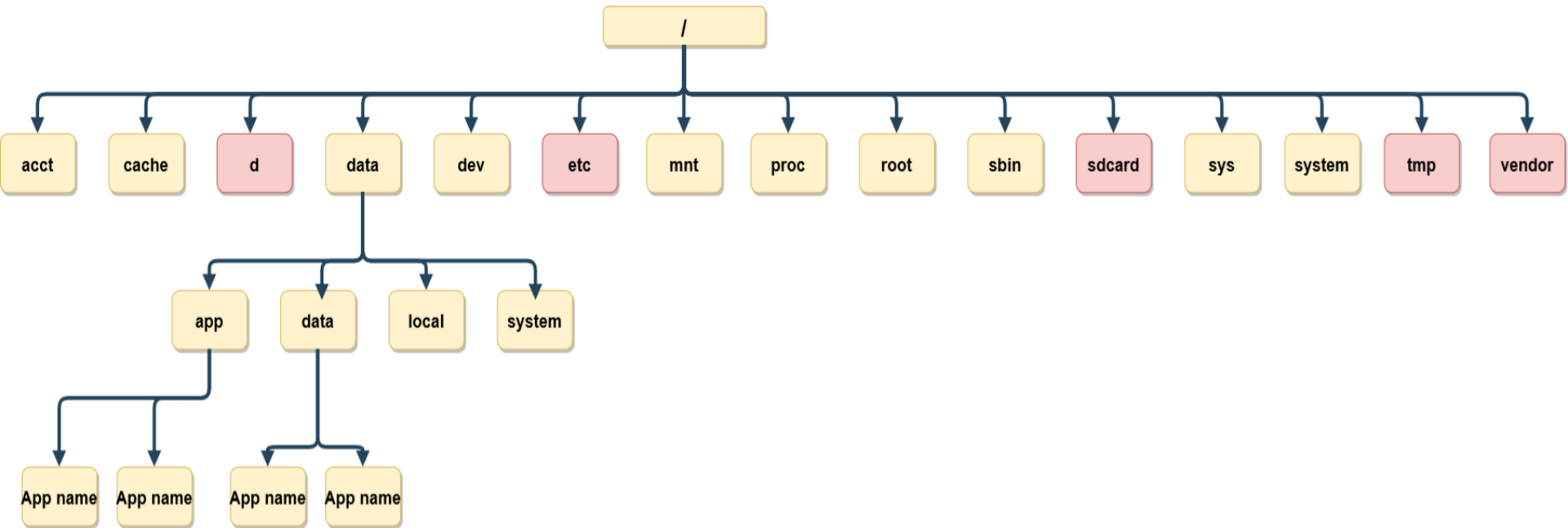
Particiones

Android

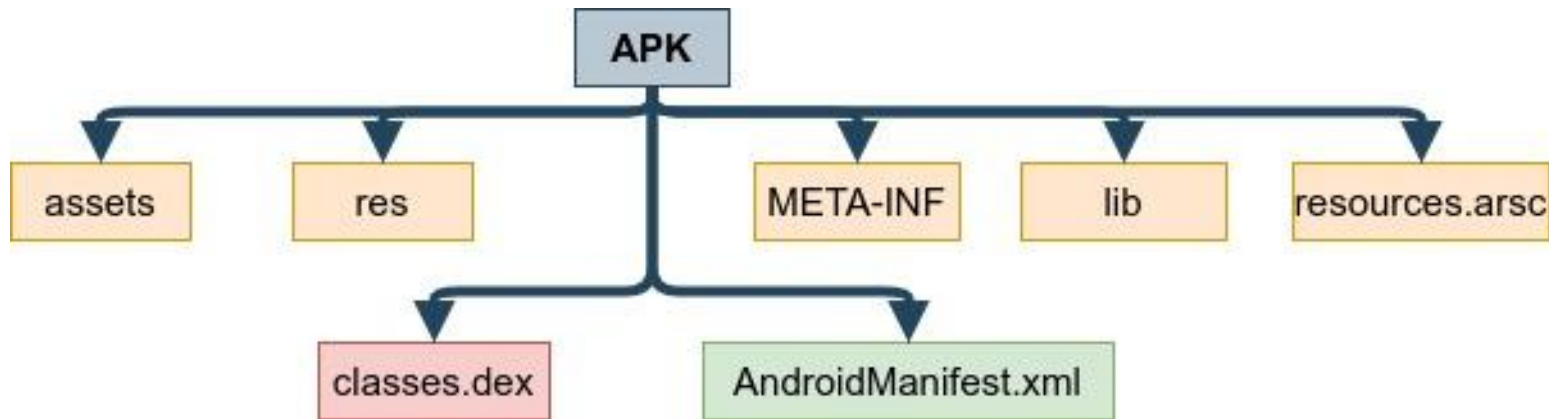
- **Cache:** para almacenar datos y componentes que son accedidos con frecuencia.
- **Misc:** para almacenar diversas opciones del sistema y aspectos relacionados con el hardware.
- **Sdcard:** esta partición no pertenece a la memoria interna del teléfono. Para almacenar documentos, imágenes, etc.
- **Sd-ext:** no es una partición estándar pero es común en las ROMs personalizadas de Android.

Sistema de ficheros

Android



Estructura de una aplicación Android



- **Android Application Package (APK):** paquete software que engloba todos los recursos relacionados con una aplicación Android. Es una variante del formato JAR de Java.
 - Extensión → *.apk*

Estructura de una aplicación Android

- **assets:** directorio con los recursos extra utilizados por la aplicación (fuentes, archivos multimedia, etc).
- **res:** directorio con los recursos Android no compilados de la aplicación (animaciones, estilos, layouts, strings, etc).
- **META-INF:** directorio con metadatos de la aplicación (certificado, firma SHA-1, lista de recursos, etc).
- **lib:** directorio donde se almacenan las librerías nativas utilizadas por la aplicación para plataformas específicas (x86, ARM, etc) → subdirectorio para cada arquitectura.

Estructura de una aplicación Android

- **resources.arsc**: directorio con recursos pre-compilados de la aplicación (cadenas de texto, estilos, etc).
- **classes.dex**: código compilado (bytecode) de la aplicación en formato Dalvik Executable (**.dex**) → ejecutado por el Android Runtime.
 - Puede ser convertido a una representación legible (Smali) desensamblando el .dex.

Estructura de una aplicación Android

```
.method public static aes256encrypt([B[B[B[B
    .locals 4
    .param p0, "ivBytes"    # [B
    .param p1, "keyBytes"   # [B
    .param p2, "textBytes"  # [B
    .annotation system Ldalvik/annotation/Throws;
        value = {
            Ljava/io/UnsupportedEncodingException;,
            Ljava/security/NoSuchAlgorithmException;,
            Ljavax/crypto/NoSuchPaddingException;,
            Ljava/security/InvalidKeyException;,
            Ljava/security/InvalidAlgorithmParameterException;,
            Ljavax/crypto/IllegalBlockSizeException;,
            Ljavax/crypto/BadPaddingException;
        }
    .end annotation

    .prologue
    .line 52
    new-instance v1, Ljavax/crypto/spec/IvParameterSpec;

    invoke-direct {v1, p0}, Ljavax/crypto/spec/IvParameterSpec;-><init>([B)V

    .line 53
    .local v1, "ivSpec":Ljava/security/spec/AlgorithmParameterSpec;
    new-instance v2, Ljavax/crypto/spec/SecretKeySpec;

    const-string v3, "AES"

    invoke-direct {v2, p1, v3}, Ljavax/crypto/spec/SecretKeySpec;-><init>([BLjava/lang/String;)V
```

Estructura de una aplicación Android

- **AndroidManifest.xml:** fichero que contiene toda la información que necesita la aplicación para su correcta instalación y ejecución:
 - Versión mínima soportada.
 - Nombre de la aplicación y versión.
 - Permisos de la aplicación que se solicitarán al usuario.
 - Librerías del sistema necesarias.
 - Componentes que incluye la aplicación → actividades servicios, etc.

Estructura de una aplicación Android

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.android.insecurebankv2" >

    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.SEND_SMS" />

    <!--
        To retrieve OAuth 2.0 tokens or invalidate tokens to disconnect a user. This disconnect
        option is required to comply with the Google+ Sign-In developer policies
    -->
    <uses-permission android:name="android.permission.USE_CREDENTIALS" /> <!-- To retrieve the account name (email) as part of sign-in: -->
    <uses-permission android:name="android.permission.GET_ACCOUNTS" /> <!-- To auto-complete the email text field in the login form with the user's emails -->
    <uses-permission android:name="android.permission.READ_PROFILE" />
    <uses-permission android:name="android.permission.READ_CONTACTS" />

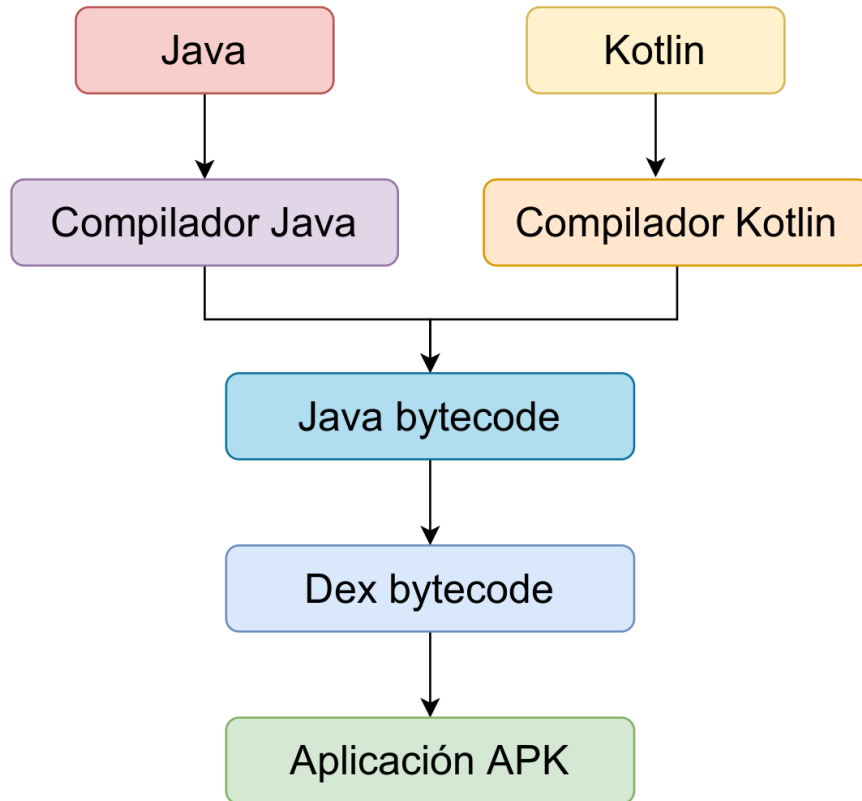
    <android:uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <android:uses-permission
        android:name="android.permission.READ_EXTERNAL_STORAGE"
        android:maxSdkVersion="18" />
    <android:uses-permission android:name="android.permission.READ_CALL_LOG" />

    <application
        android:allowBackup="true"
        android:icon="@mipmap/ic_launcher"
        android:label="@string/app_name"
        android:theme="@android:style/Theme.Holo.Light.DarkActionBar">
        <!--
            android:theme="@style/AppTheme"-->
        <activity
            android:name=".LoginActivity"
            android:label="@string/app_name" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
```

Creación de ficheros *.apk*

Android



- El código fuente escrito en lenguaje Java o Kotlin es compilado produciendo archivos **.class** con el bytecode de Java → se almacenan/empaquetan en un fichero **.jar**
- El bytecode de Java se transforma en bytecode **.dex** que es el código que ejecutará el Android Runtime o la máquina virtual Dalvik.
- Finalmente, este fichero **.dex** junto con los distintos recursos de la aplicación, el AndroidManifest, etc, se comprime en formato **.zip** → **.apk**
- Si se desea publicar la aplicación en Google Play, esta debe firmarse con un certificado.