DGTIC UNAM CERT

2do Coloquio de Proyectos de Becarios en Seguridad Informática

Guía para el análisis de vulnerabilidades en aplicaciones móviles

Juan Alberto Camacho Bolaños
Félix Alejandro Hernández Fuentes

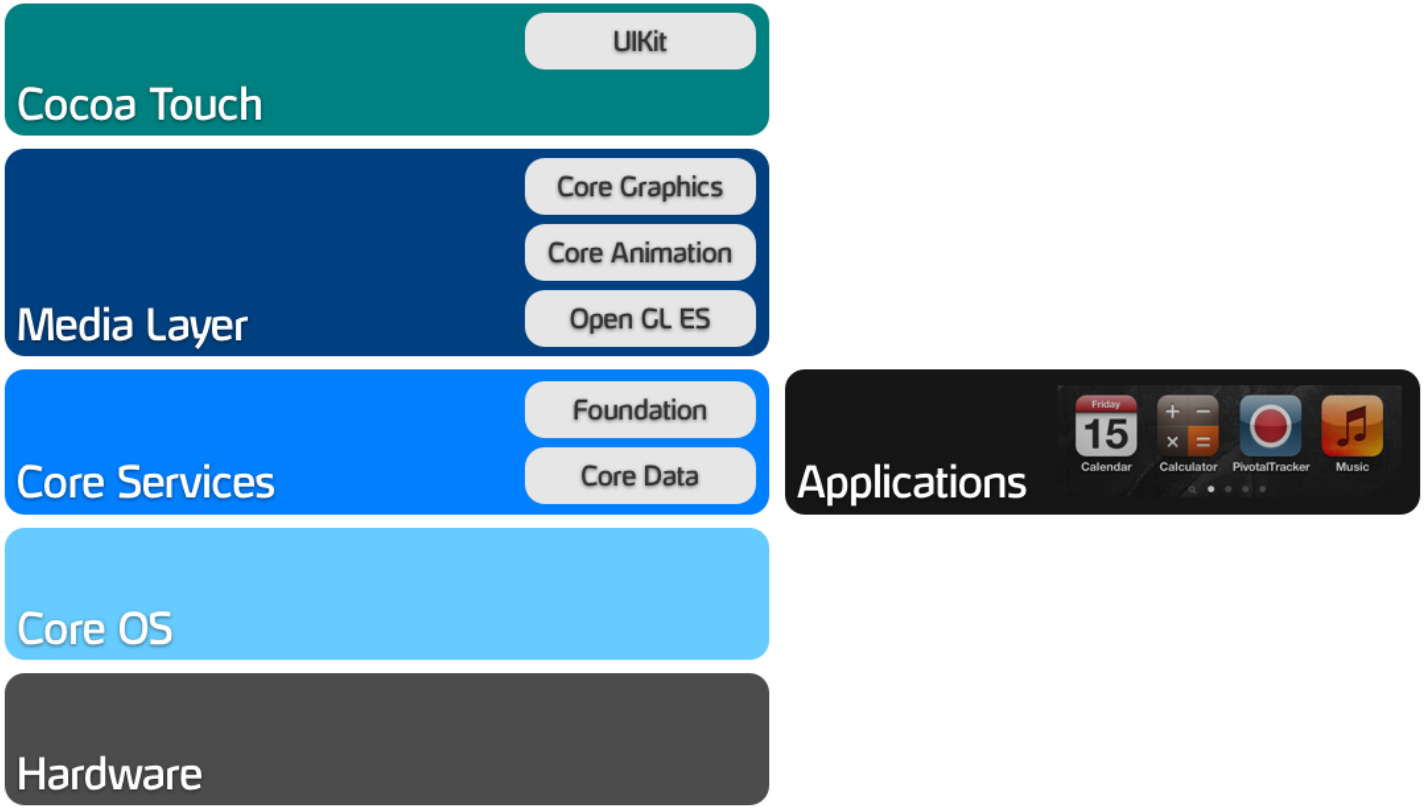
Objetivo

Top 10 de vulnerabilidades en aplicaciones móviles OWASP, 2014

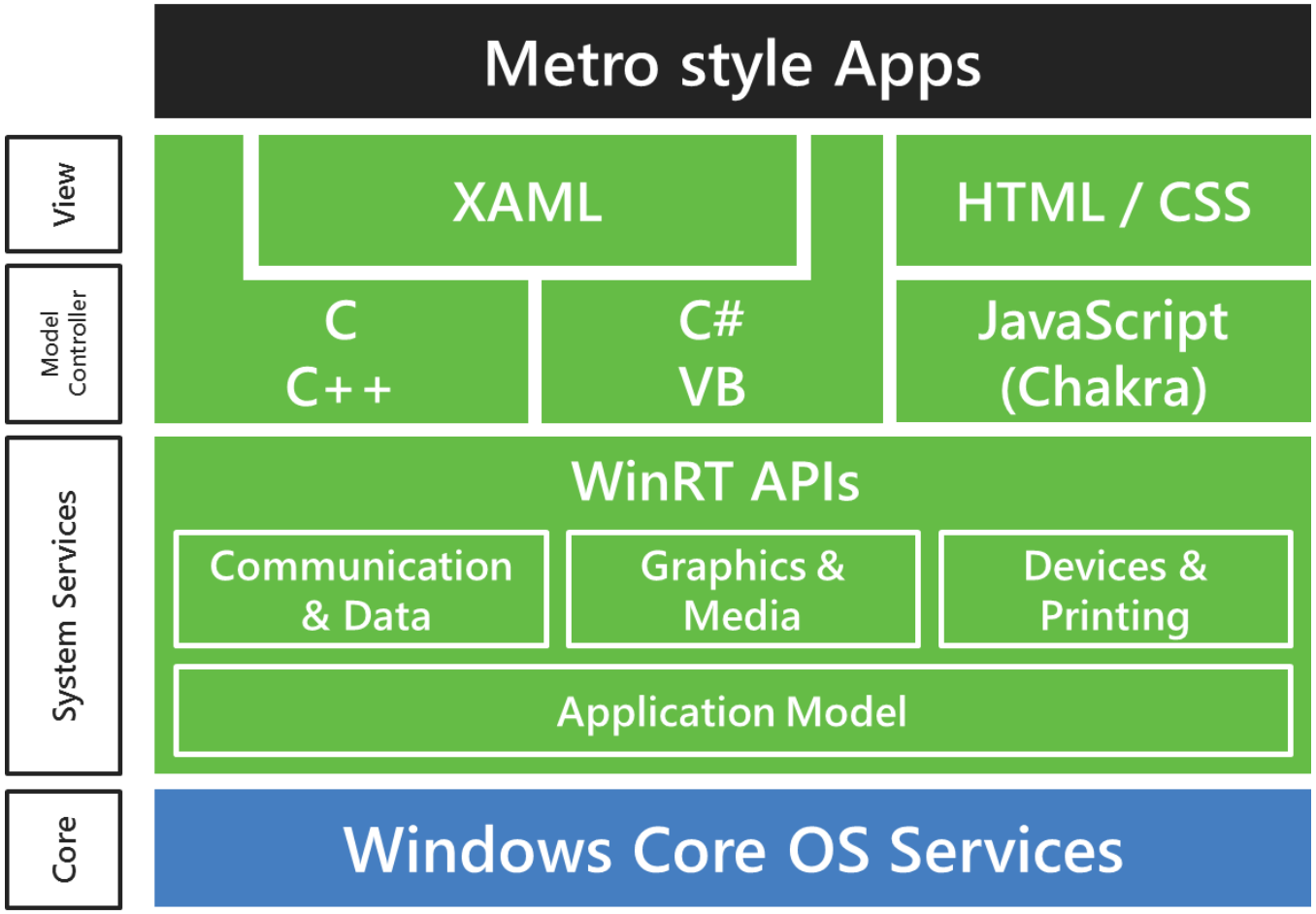
1. Controles insuficientes del lado del servidor
2. Almacenamiento inseguro de datos
3. Protección insuficiente en la capa de transporte
4. Fuga de datos no intencional
5. Mecanismos de autenticación y autorización deficientes
6. Uso de algoritmos de cifrado que han sido comprometidos
7. Inyecciones del lado del cliente
8. Decisiones de seguridad a través de entradas no confiables
9. Mal manejo de sesiones
10. Falta de protección en binarios

Sistema Operativo Android

Sistema Operativo iOS



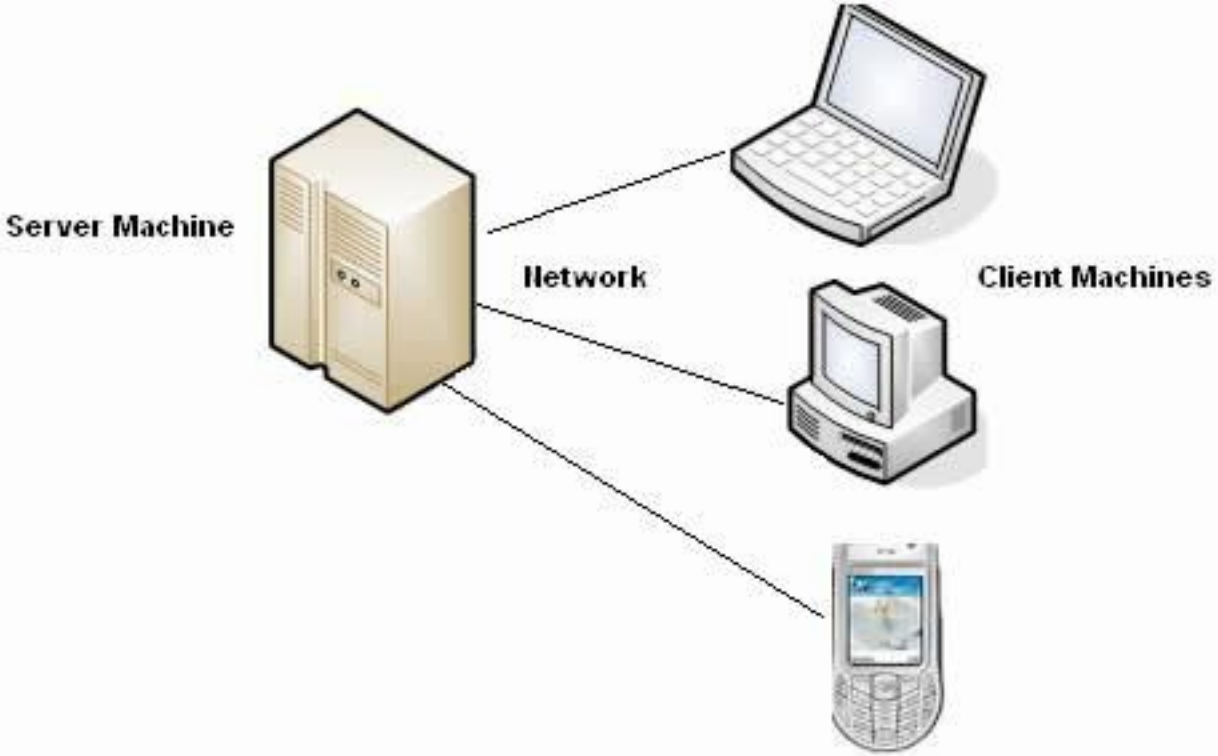
Sistema Operativo Windows Phone



Guía de análisis de vulnerabilidades

- El ciclo de vida de una aplicación móvil depende principalmente de:
  - Servidor donde se almacenará la información de la aplicación
  - Canal de comunicación
  - Aplicación móvil

Las aplicaciones utilizan una arquitectura cliente servidor



Guía para el análisis de vulnerabilidades

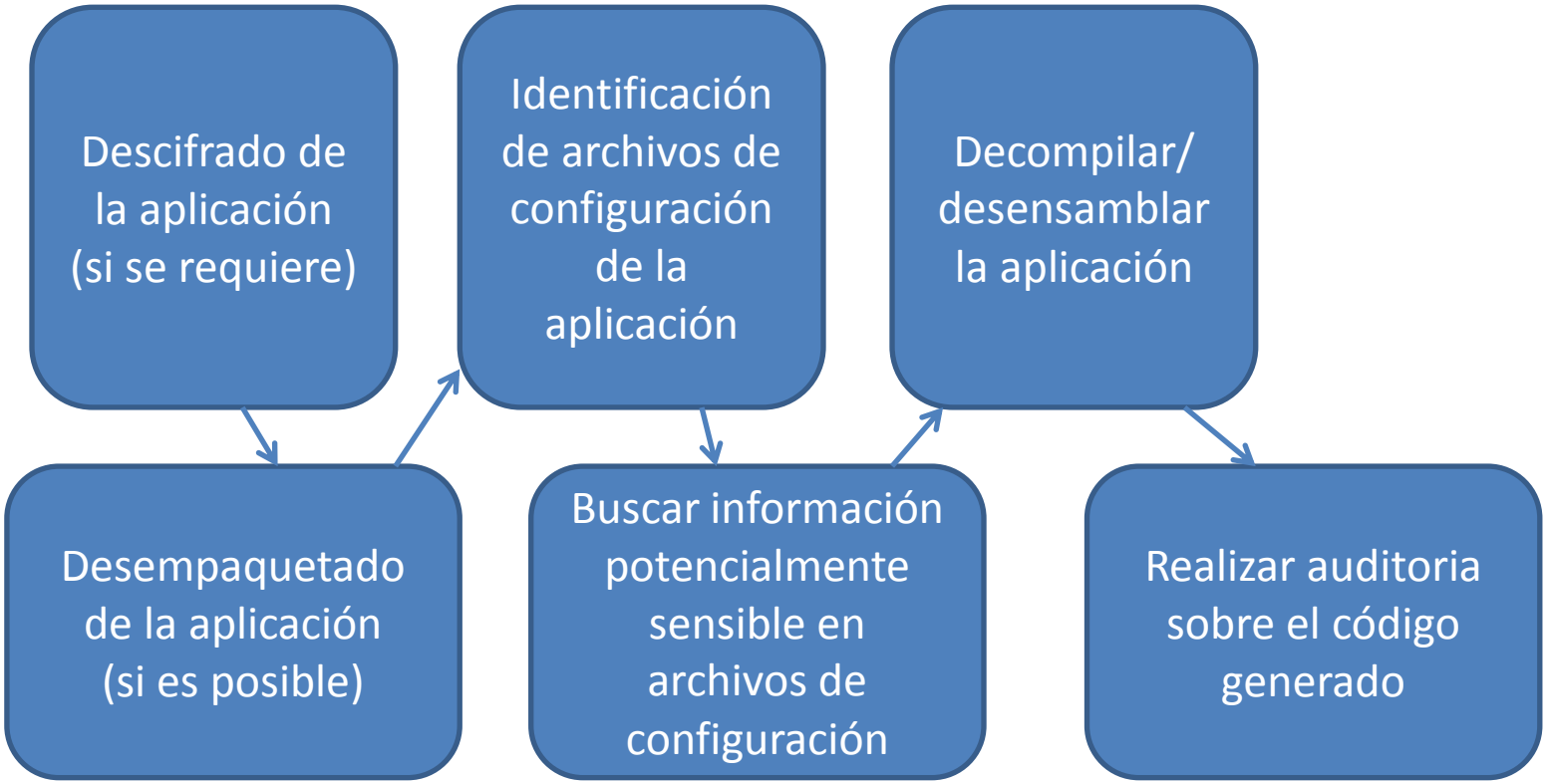
Creación de un laboratorio de pruebas con todas las herramientas necesarias

Análisis estático

Análisis dinámico

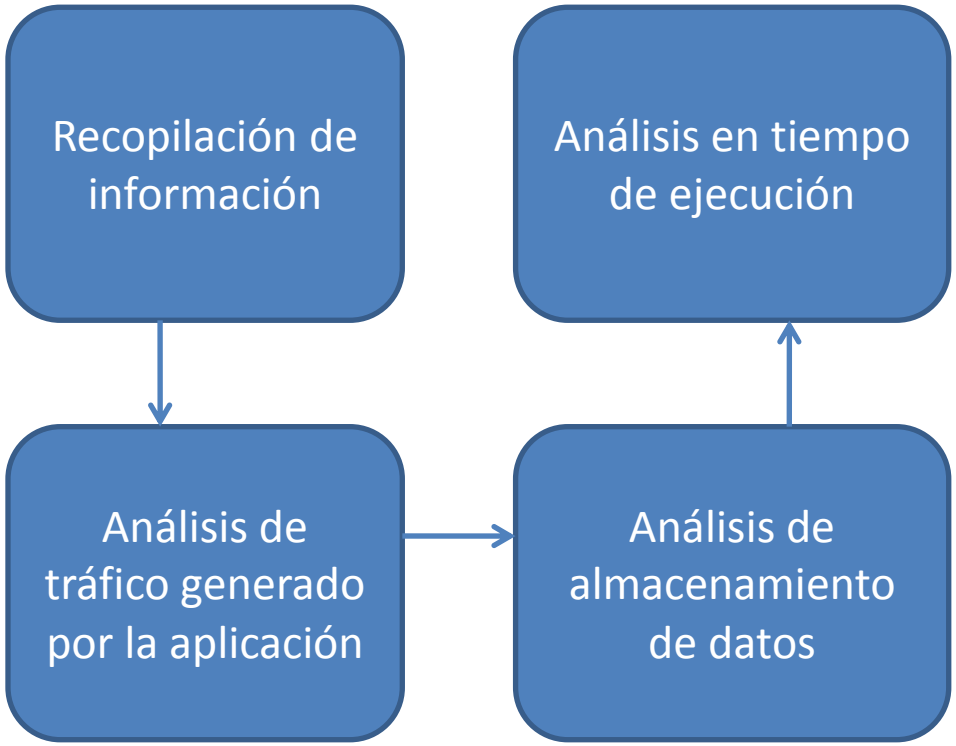
Guía para el análisis de vulnerabilidades

- Análisis estático



Guía para el análisis de vulnerabilidades

- Análisis dinámico



- ✓Interacción con el sist. de archivos
- ✓Inspeccionar objetos en memoria
- ✓Llamadas a funciones y métodos
- ✓Reemplazar variables y métodos
- ✓Buffer overflow
- ✓Inyecciones del lado del cliente (XML, XSS, SQL)

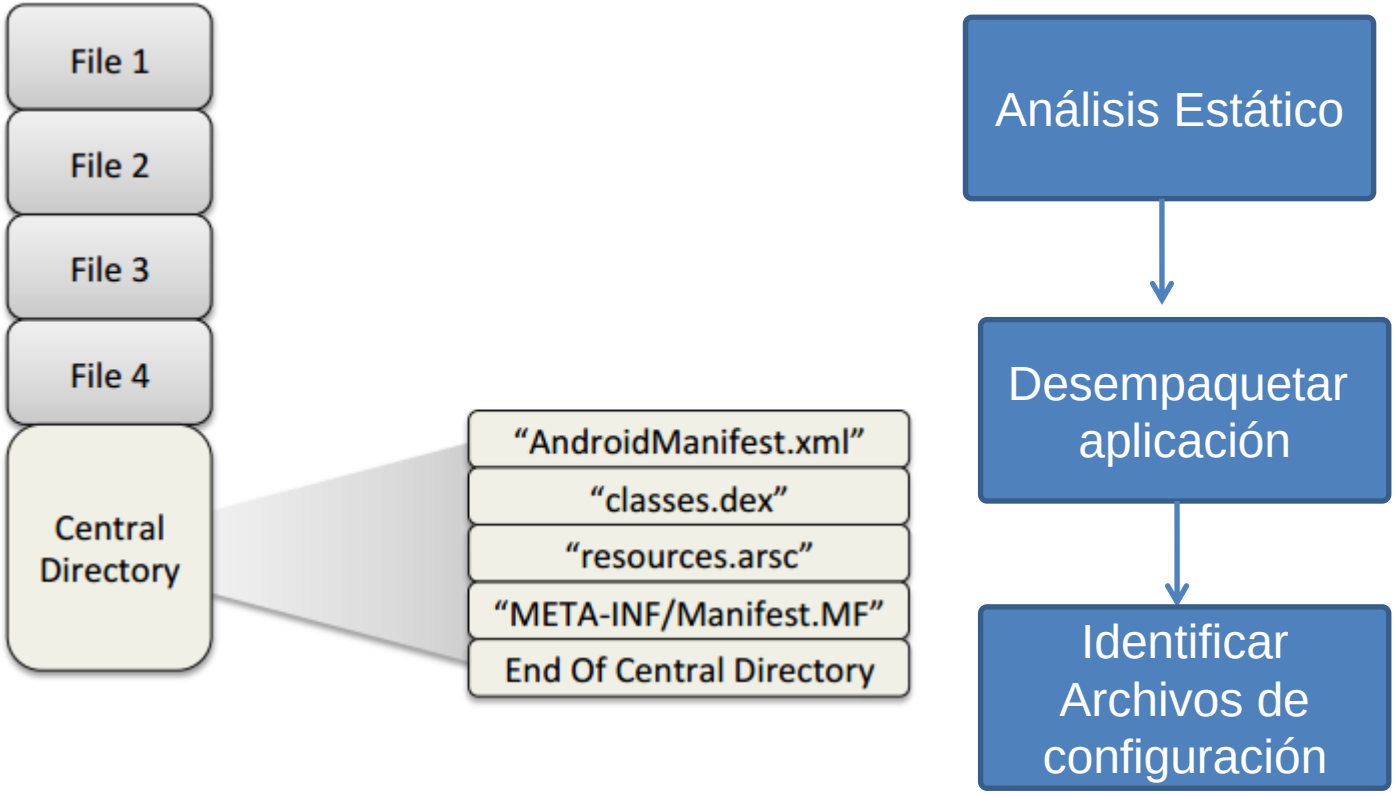
Demostración

- Android security bug 8219321, “Master key”
- CVE-2013-4787

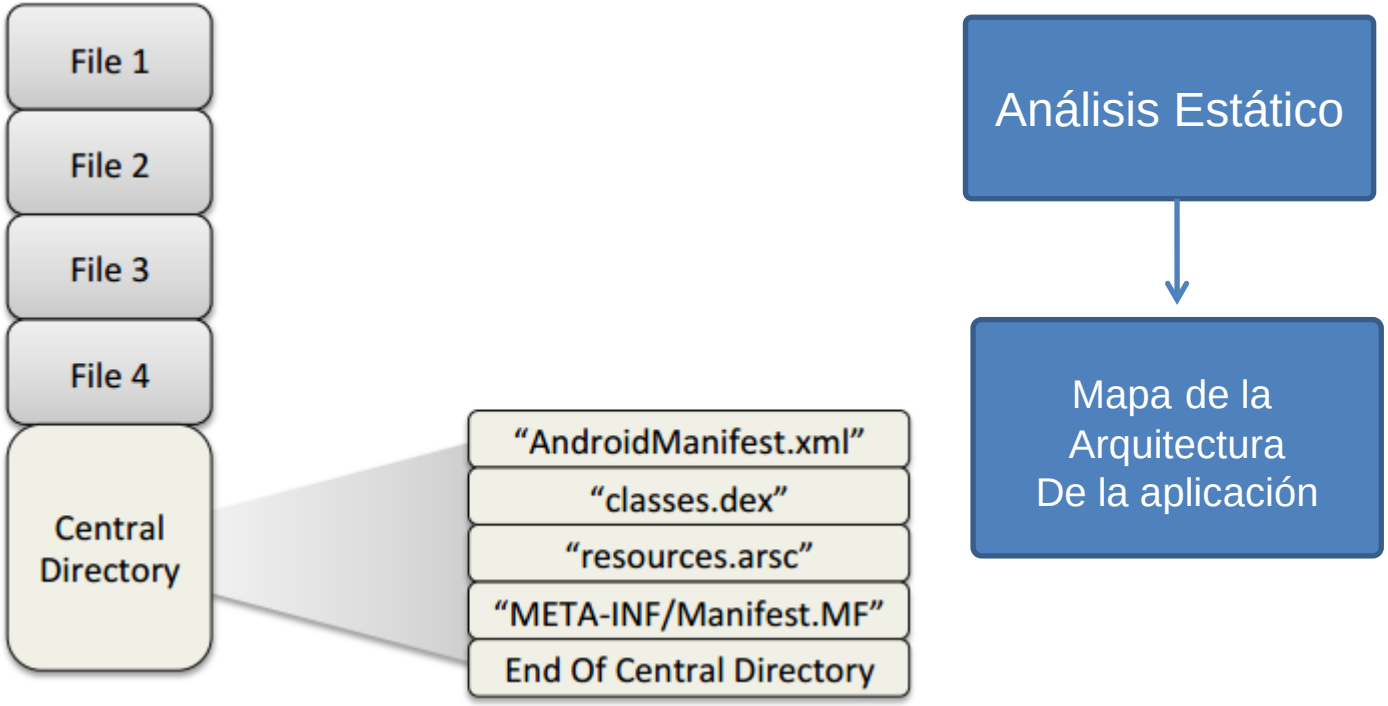
- Las firmas criptográficas de las aplicaciones no son debidamente comprobadas, lo que permite a un atacante ejecutar código arbitrario a través de un APK modificado de tal forma que no se viola la firma criptográfica.

- Versiones afectadas: desde Android 1.6 (Donut) hasta 4.2 (Jelly Bean)

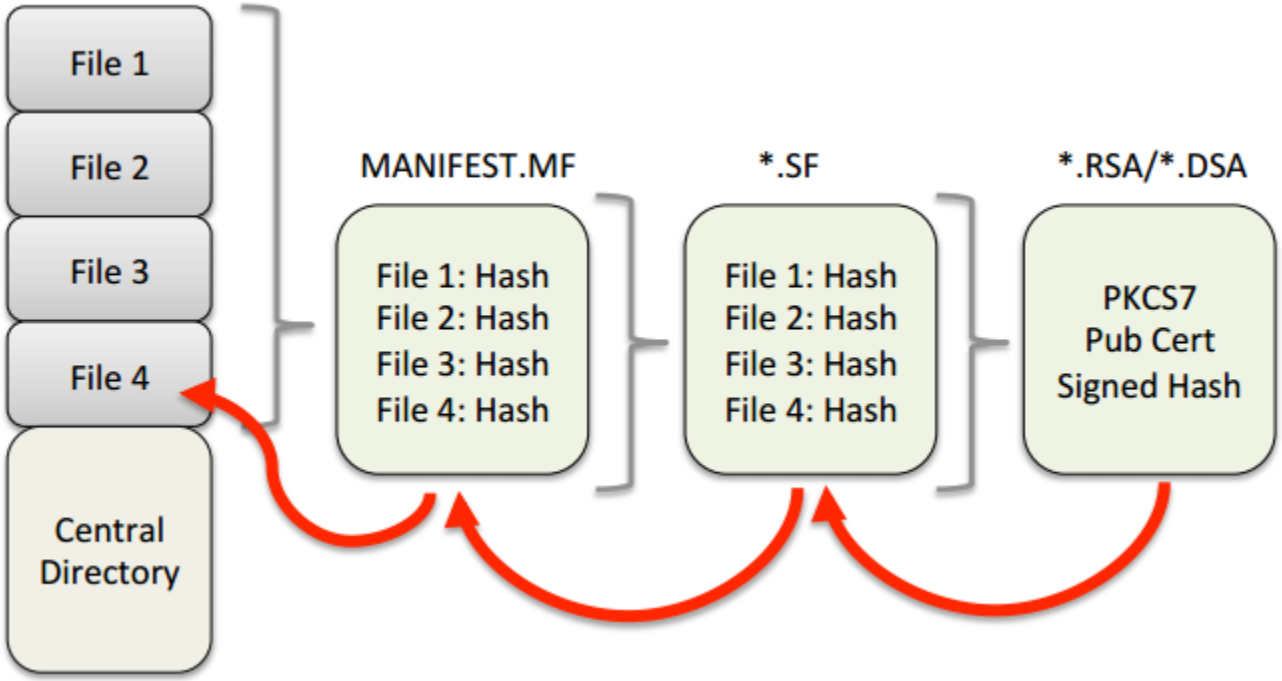
Estructura del APK como archivo ZIP



Estructura del APK como archivo ZIP

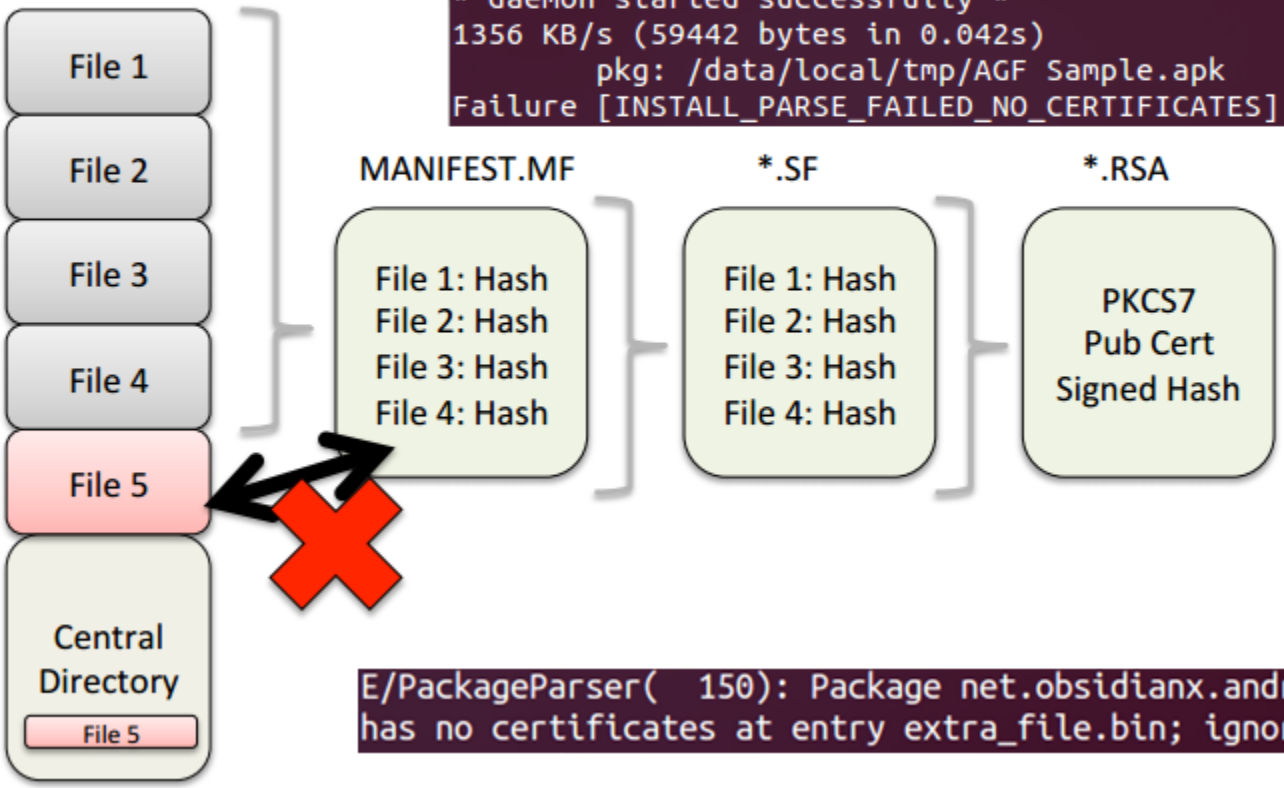


Verificación de firmas de la aplicación



Verificación fallida

```
root@ubuntu:/home/analista/adt-bundle/sdk/platform-tools#
./adb install AGF\ Sample.apk
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
1356 KB/s (59442 bytes in 0.042s)
        pkg: /data/local/tmp/AGF Sample.apk
Failure [INSTALL_PARSE_FAILED_NO_CERTIFICATES]
```



Análisis Dinámico

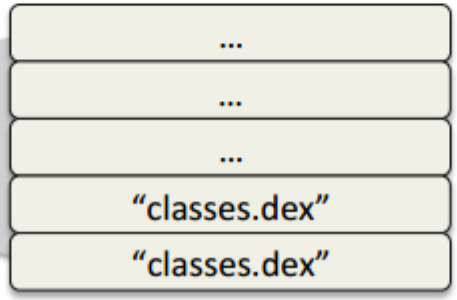
Almacenamiento Inseguro de datos

```
E/PackageParser(  150): Package net.obsidianx.android.gameframe
has no certificates at entry extra_file.bin; ignoring!
```

Duplicación de entradas

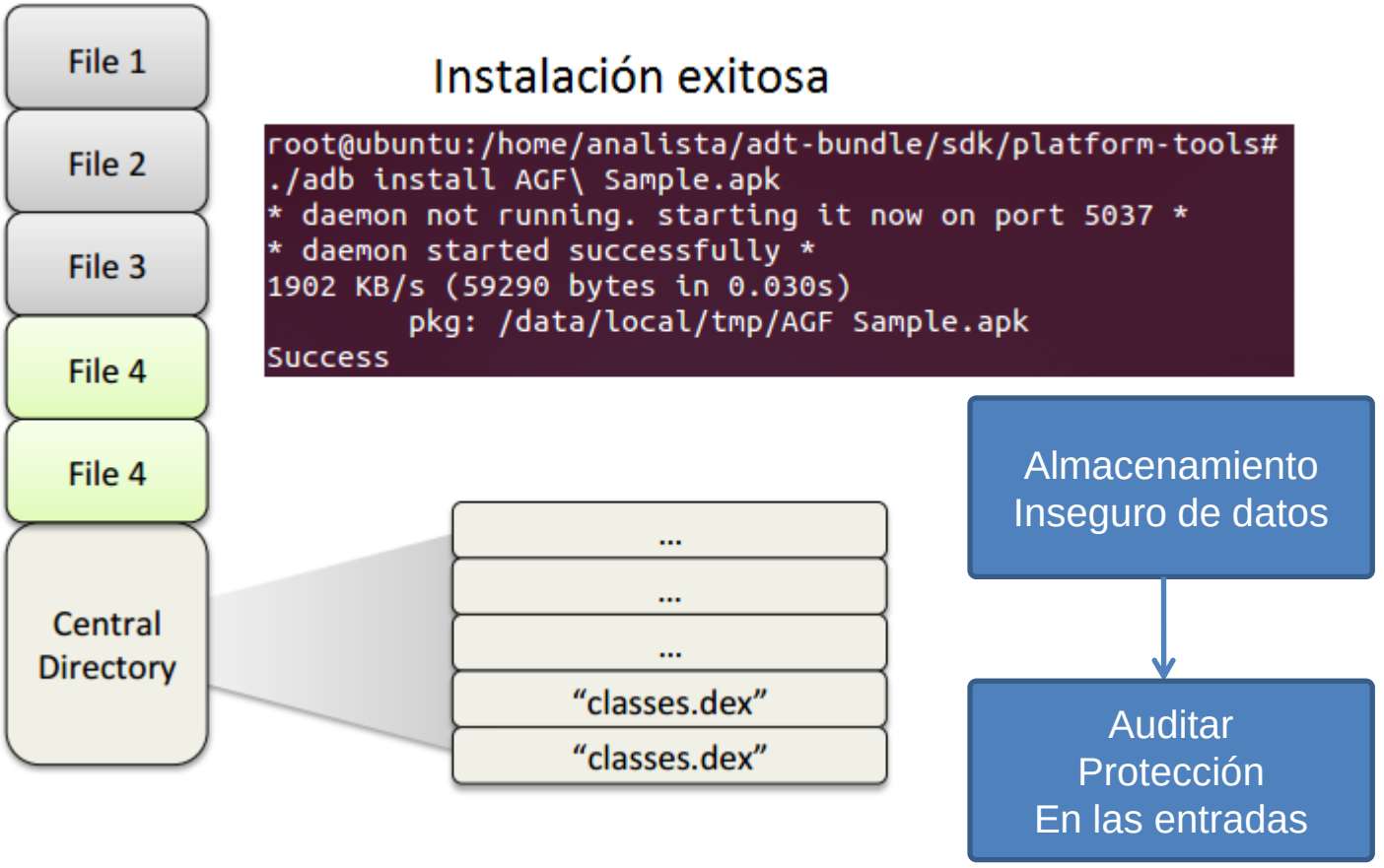
Instalación exitosa

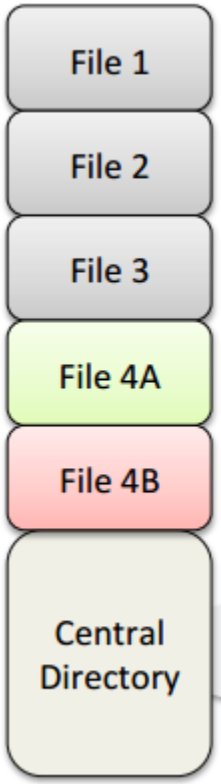
```
root@ubuntu:/home/analista/adt-bundle/sdk/platform-tools#
./adb install AGF\ Sample.apk
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
1902 KB/s (59290 bytes in 0.030s)
        pkg: /data/local/tmp/AGF Sample.apk
Success
```

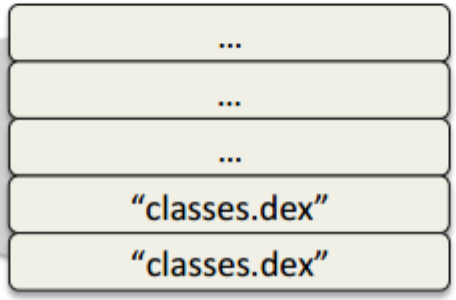


Almacenamiento Inseguro de datos

Duplicación de entradas







Verificación de la firma exitosa

```
root@ubuntu:/home/analista/adt-bundle/sdk/platform-tools#
jarsigner -verify AGF\ Sample.apk
jar verified.
```

La instalación no se lleva a cabo

```
root@ubuntu:/home/analista/adt-bundle/sdk/platform-tools#
./adb install AGF\ Sample.apk
1336 KB/s (57772 bytes in 0.042s)
        pkg: /data/local/tmp/AGF Sample.apk
Failure [INSTALL_PARSE_FAILED_NO_CERTIFICATES]
```

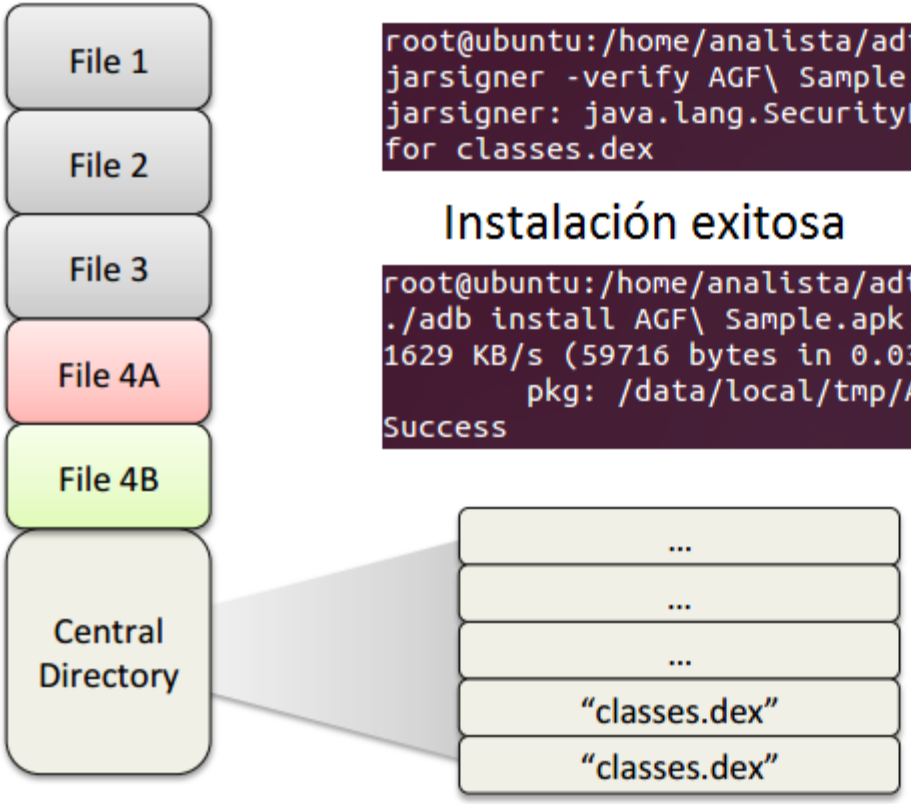
Almacenamiento Inseguro de datos

Fallo al verificar la firma

```
root@ubuntu:/home/analista/adt-bundle/sdk/platform-tools#
jarsigner -verify AGF\ Sample.apk
jarsigner: java.lang.SecurityException: SHA1 digest error
for classes.dex
```

Instalación exitosa

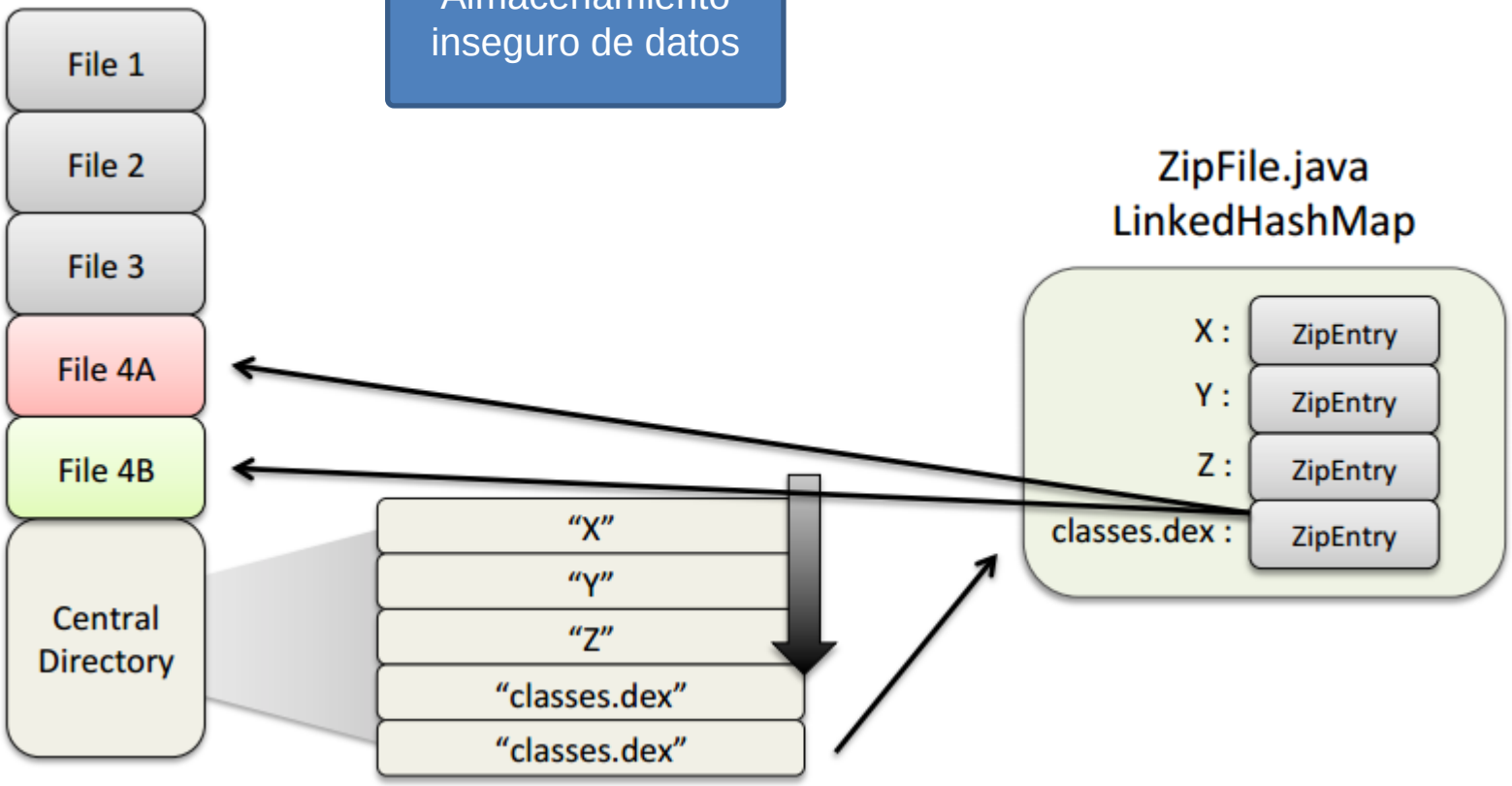
```
root@ubuntu:/home/analista/adt-bundle/sdk/platform-tools#
./adb install AGF\ Sample.apk
1629 KB/s (59716 bytes in 0.035s)
        pkg: /data/local/tmp/AGF Sample.apk
Success
```

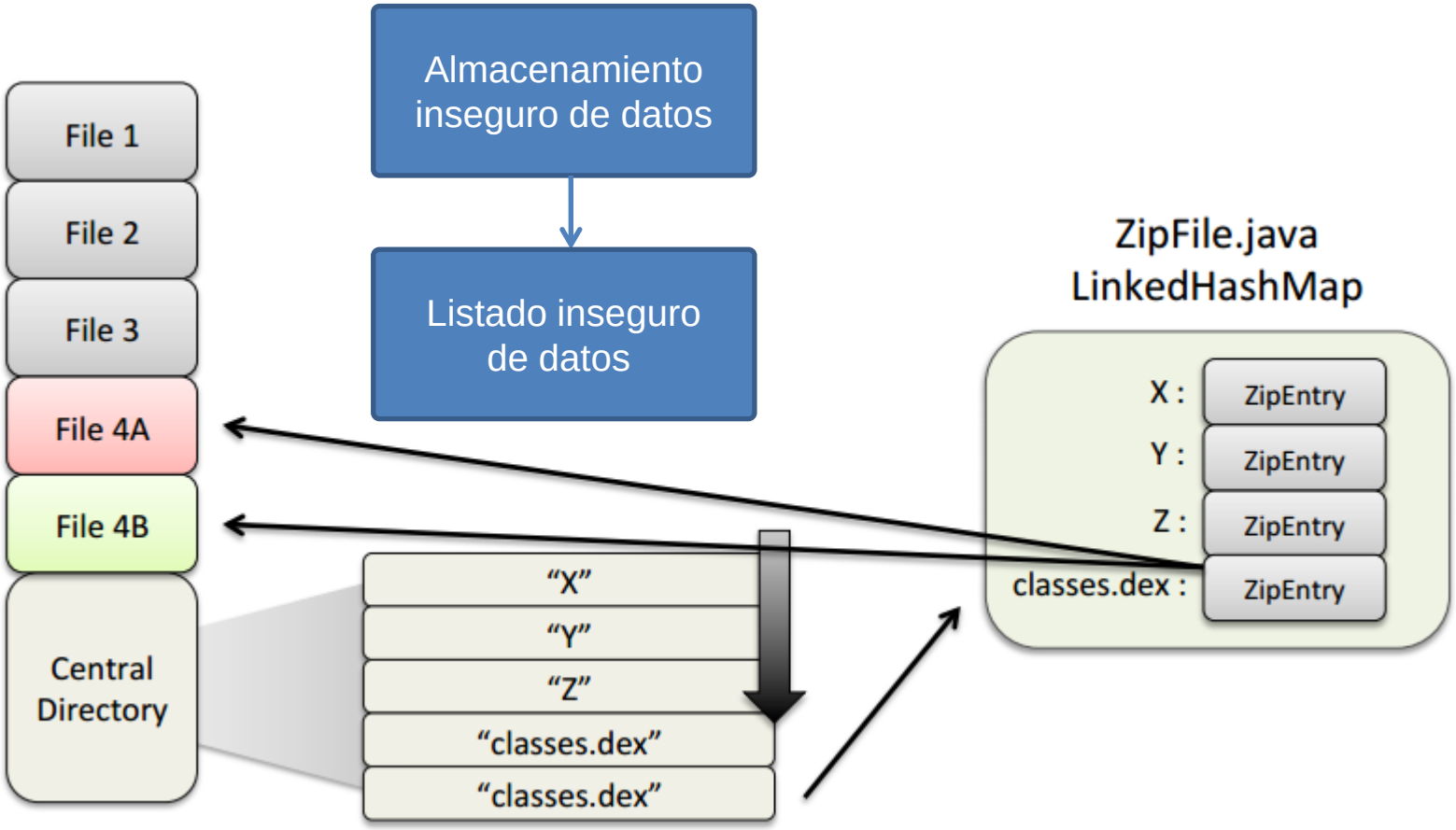


Almacenamiento inseguro de datos

Auditar protección en las entradas

Almacenamiento inseguro de datos




Almacenamiento inseguro de datos
Listado inseguro de datos
File 1
File 2
File 3
File 4A
File 4B
Central Directory
"X"
"Y"
"Z"
"classes.dex"
"classes.dex"
ZipFile.java
LinkedHashMap
X :
Y :
Z :
classes.dex :
ZipEntry
ZipEntry
ZipEntry
ZipEntry