Android Pentesting

Cristian Rodríguez

01/12/2018

Sobre mí...

- Ingeniería en Computación. (2007)
- OSCP. (2015)
- Maestría en Ciberseguridad. (2017)
- Penetration Tester (4+ años)

Agenda

- Porqué Mobile Pentesting?
- Porqué Android?
  - Modelo de Seguridad.
  - Android Package Kit (apk).
- Análisis Estático vs. Análisis Dinámico.
- OWASP Mobile Top 10
  - M1 – Insecure Platform Usage.
  - M2 – Insecure Data Storage.
  - M3 – Insecure Communication.
- Conclusión.

Porqué Mobile Pentesting?

- Cada vez más queremos tener todo al alcance de nuestras manos:
  - Transporte, alimentación, entrenemiento, banca, salud, etc.

Porqué Android?

- Quienes aquí utilizan Android?

Operating System	1Q18 Units	1Q18 Market Share (%)	1Q17 Units	1Q17 Market Share (%)
Android	329,313.9	85.9	325,900.9	86.1
iOS	54,058.9	14.1	51,992.5	13.7
Other OS	131.1	0.0	607.3	0.2
Total	**383,503.9**	**100.0**	**378,500.6**	**100.0**

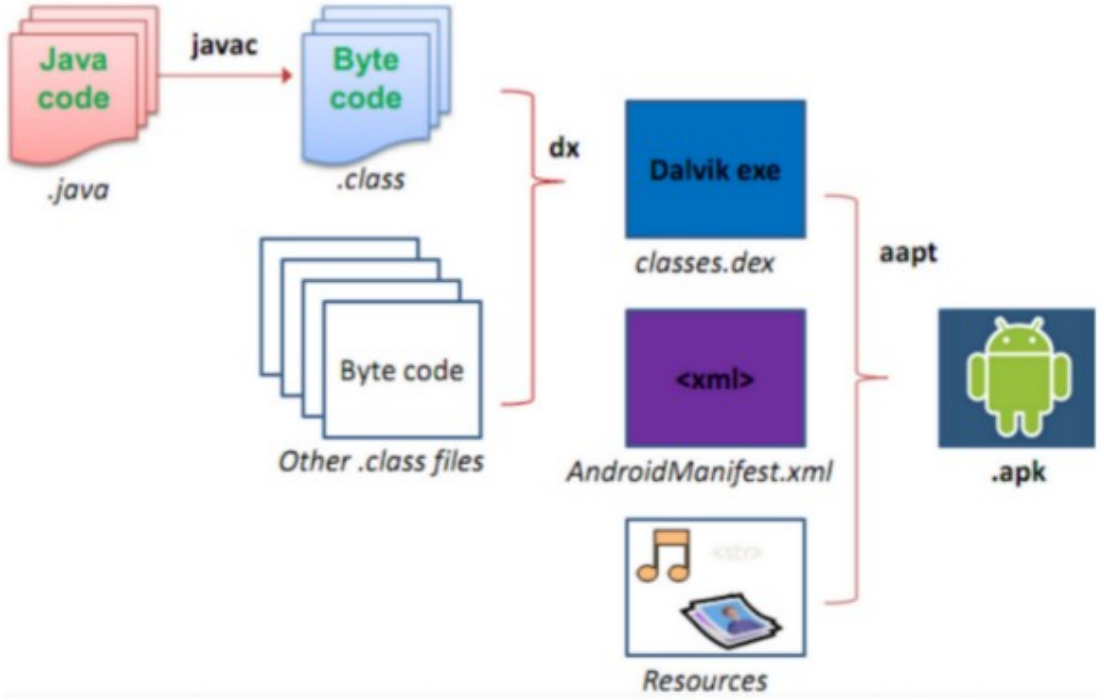
Source: Gartner (May 2018)

Android

- Modelo de Seguridad:
  - SO Robusto y establecido (primera versión basado en el Kernel de Linux 2.6.27).
  - DALVIK VM individuales.
    - Cada app corre aislada es su VM (sandbox).
  - Usuario único por aplicación.
  - Controles de seguridad a nivel de OS y aplicación.
  - Apps firmadas digitalmente.

Android

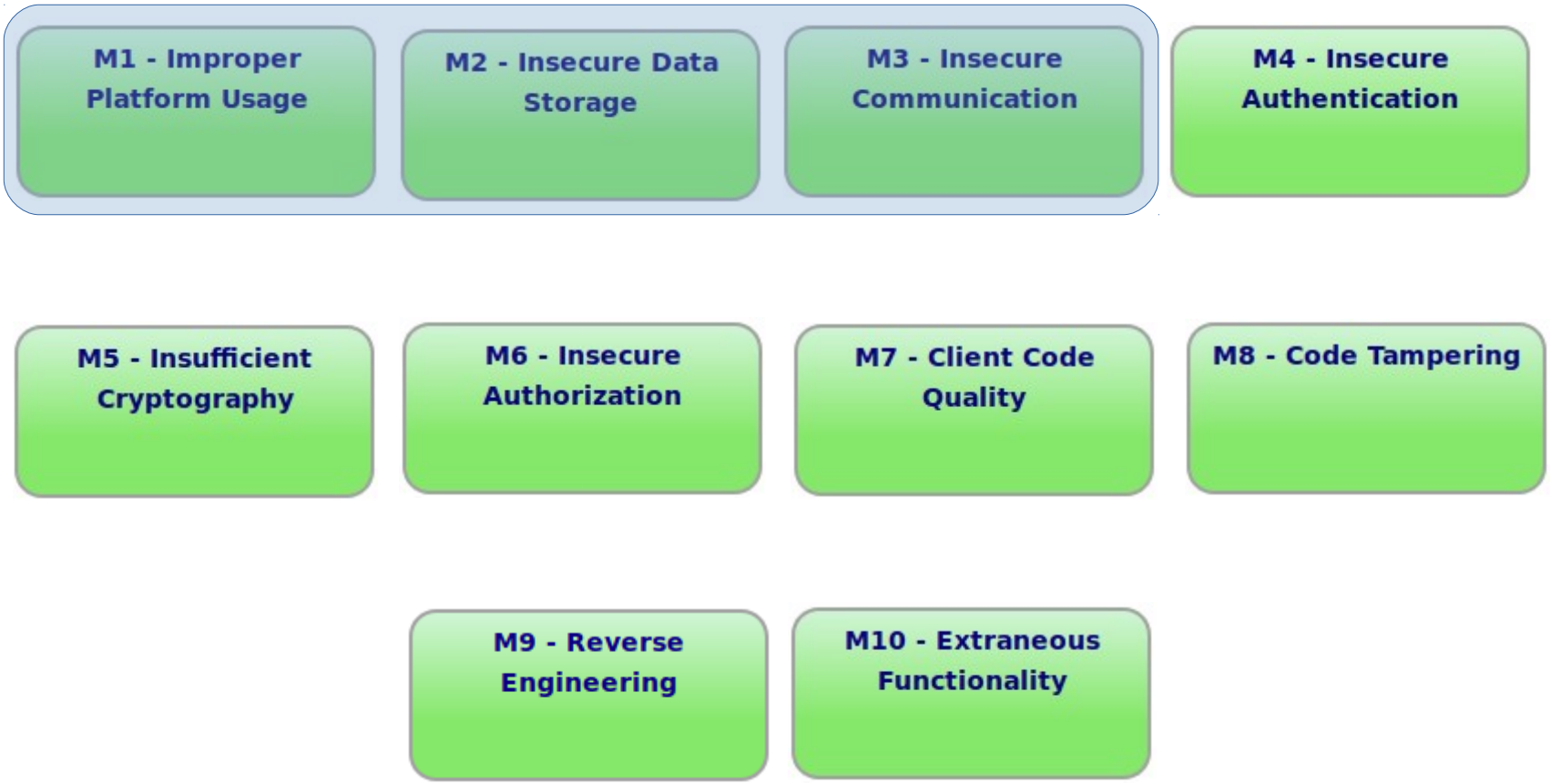
- Android Package Kit (apk):



Análisis Estático vs Dinámico

- **Estático:** Se analiza el apk sin instalarla ni ejecutarla.
  - Ingeniería reversa, análisis de archivos de configuración, código descompilado, ofuscación, etc.
- **Dinámico:** Se analiza la aplicación al instalarla y ejecutarla.
  - Analizar folders, archivos, bases de datos locales, comunicación, componentes, etc.

OWASP Mobile Top 10

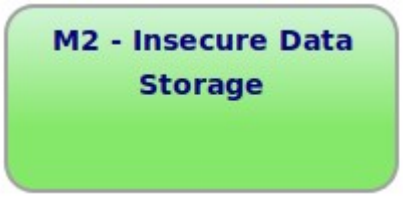


M1 – Improper Platform Usage.

- **Descripción**: Cubre el mal uso de la plataforma o no utilizar correctamente controles de seguridad existentes.

- **Herramientas**:
  - Apktool (Androidmanifest.xml)
    - Activities, permissions, allowBackup, debuggable.
  - Drozer framework.

M2 – Insecure Data Storage.



- **Descripción**: Cubre el almacenamiento inseguro de datos o la fuga no intencional de los mismos.

- **Herramientas**:
  - d2j-dex2jar
  - jd-gui
  - sqlite3
  - logcat

M3 – Insecure Communication.

- **Descripción**: Cubre configuraciones incorrectas a nivel de SSL/TLS.
  - Pinning.
  - Versiones vulnerables.
  - Negociación débil.

- **Herramientas**:
  - Burpsuite.
  - Frida.
  - SSLyze/SSL Labs

Conclusión

- Los dispositivos móviles toman cada vez más protagonismo en nuestra vida digital.
- Garantizar que los canales de comunicación y aplicaciones móviles sean seguras es de vital importancia para la estrategia de Ciberseguridad.

Gracias

https://securitygrind.com/blog/