Unboxing Android

Who are we?

Eve Kilel @eve_kilel Information Security Analyst	Laura_Tich @_71cH Cyber Security Consultant

@shehacks_ke

Reverse Engineering

The process by which a man-made object is deconstructed to reveal its designs, architecture, or to extract knowledge from the object.

Why this Session

- To understand mobile app security.
- To spur interest in reverse engineering.
- Because we like to break things.

OWASP Top 10 Mobile Risks

● Weak Server Side Controls ● Insecure Data Storage ● Insufficient Transport Layer Protection ● Unintended Data Leakage ● Poor Authorization and Authentication	● Broken Cryptography ● Side Injection ● Security Decisions Via Untrusted Inputs ● Improper Session Handling ● Lack of Binary Protections

Role of Reverse Engineering

- Unavailability of source code triggers the need to reverse engineer binaries as well as examine other file types in order to understand how they work and analyze their weak points.
- By learning how an app is supposed to function, testers can find the variances that produce vulnerabilities. This step is crucial to ensure accurate and complete test coverage.

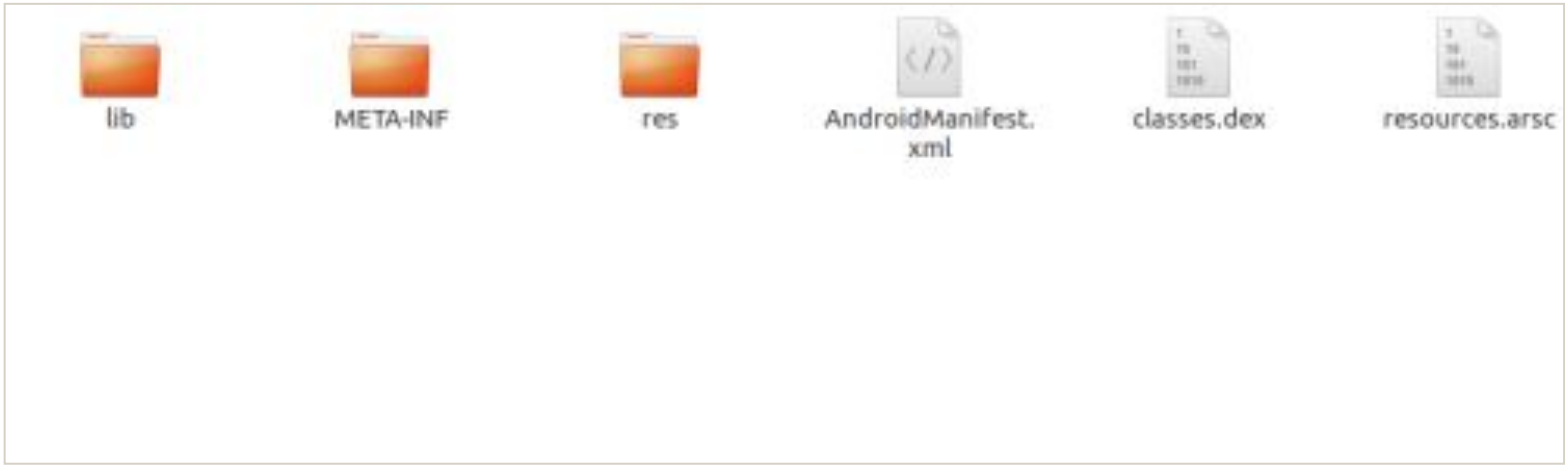
Reverse Engineering Process

- The tester must also analyze all levels from a systems view down to individual functions which includes how the app interacts with its processing and networking environment, the trust boundaries between components, and relevant lines of code. The process can uncover malware hidden in a seemingly legitimate application.
- Some vulnerabilities are more visible in binary code than in source, so reverse engineering will find them first.

Reverse Engineering Process

- In order to start the reversing process the APK file of the target application is needed. Usually the client is responsible to provide this file to the penetration tester.

APK Files


lib
META-INF
res
AndroidManifest.
xml
classes.dex
resources.arsc


WAKE UP!
IT'S DEMO TIME
memegenerator.net

TOOLS!!

- Apktool
- D2jar
- Introducing Frida

DBI

DBI (Dynamic Binary Instrumentation) is a technique for analyzing running processes.

Involves injecting instrumentation code into a running process.

What can you do with DBI?

- Access process memory
- Overwrite functions while the application is running
- Call functions from imported classes
- Find object instances on the heap and use them
- Hook, trace and intercept functions etc.


BUT...
WHAT AM I SUPPOSE TO DO NOW?
quickmeme.com

How do you protect an app code?

Apk Protection Techniques

- Code obfuscation aims to make the application’s code difficult to understand even if an attacker disassembles it, by replacing classes, fields and methods with random short names. The code will become less readable and hard to follow; hence increasing the time and resources needed by an attacker.

Apk Protection Techniques

- Android packers are able to encrypt an original classes.dex file, decrypt the dex file to memory at runtime, and then execute via DexClassLoader

Apk Protection Techniques

- Android Protectors encrypt the original classess.dex files


ANY QUESTIONS ???
memecrunch.com