Mobile App Reverse Engineering Why, What & the How's?

Karan Sharma (@_R00T_)

whoami

Security Consultant

Penetration tester (Web/Mobile)

Insert some certificates here [OSCP, eWPTX]

Cricket/Pool

What we will cover

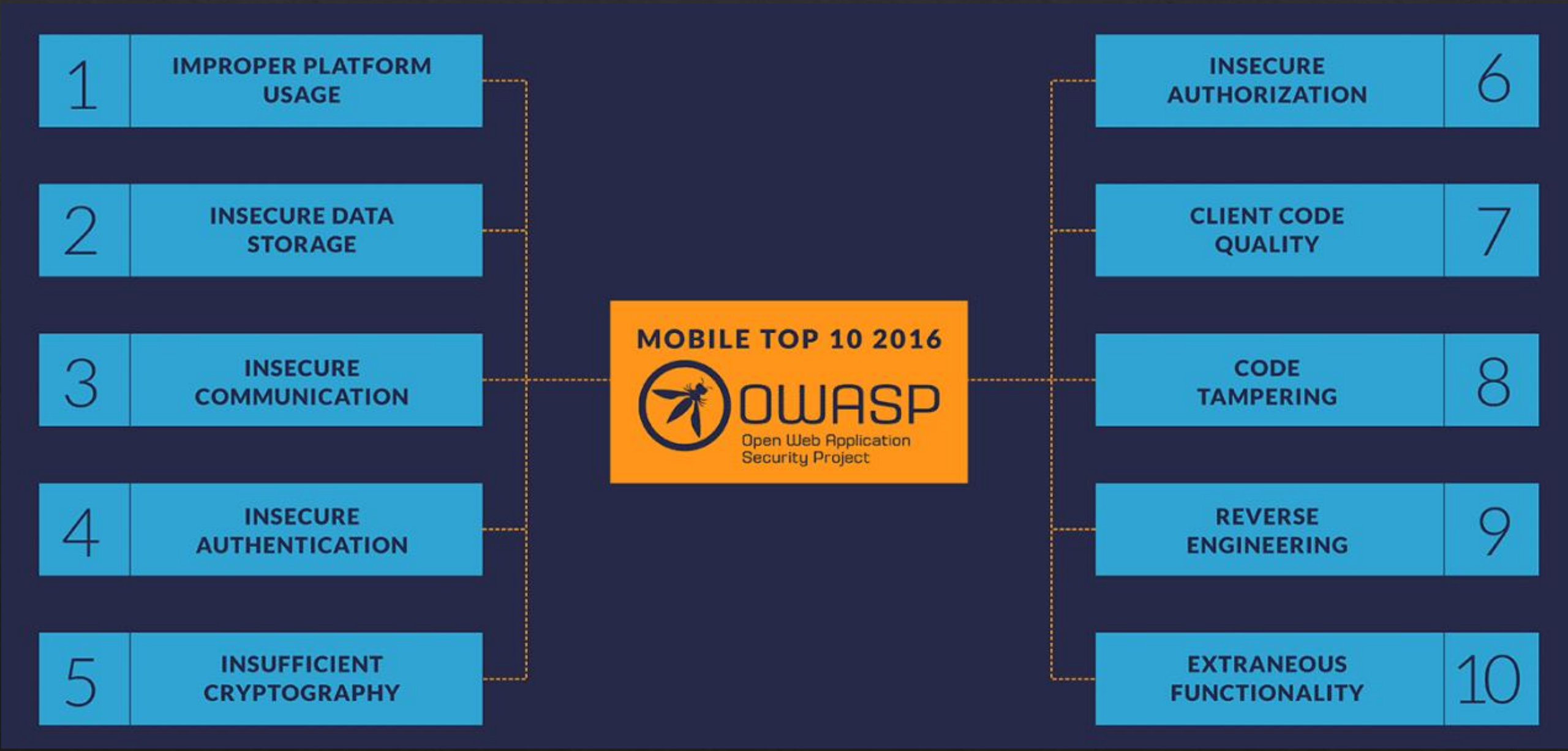
- We will only cover Android OS
- Android Architecture (crash course)
- Tools to reverse engineer an Android app
- APK compilation and decomplication process
- What to do to protect your app

Why should I do this?

- To know what is inside your application before you release it on Google Play Store or Apple's App Store.

- So you know if you are leaving any treasure inside your source code e.g. hard coded API keys, secrets, tokens, 'TO DO' comments, IP (intellectual property), backend server IPs and credentials.

- What techniques and tools an attacker can use to steal your information or break into your app.



What is Reverse Engineering?

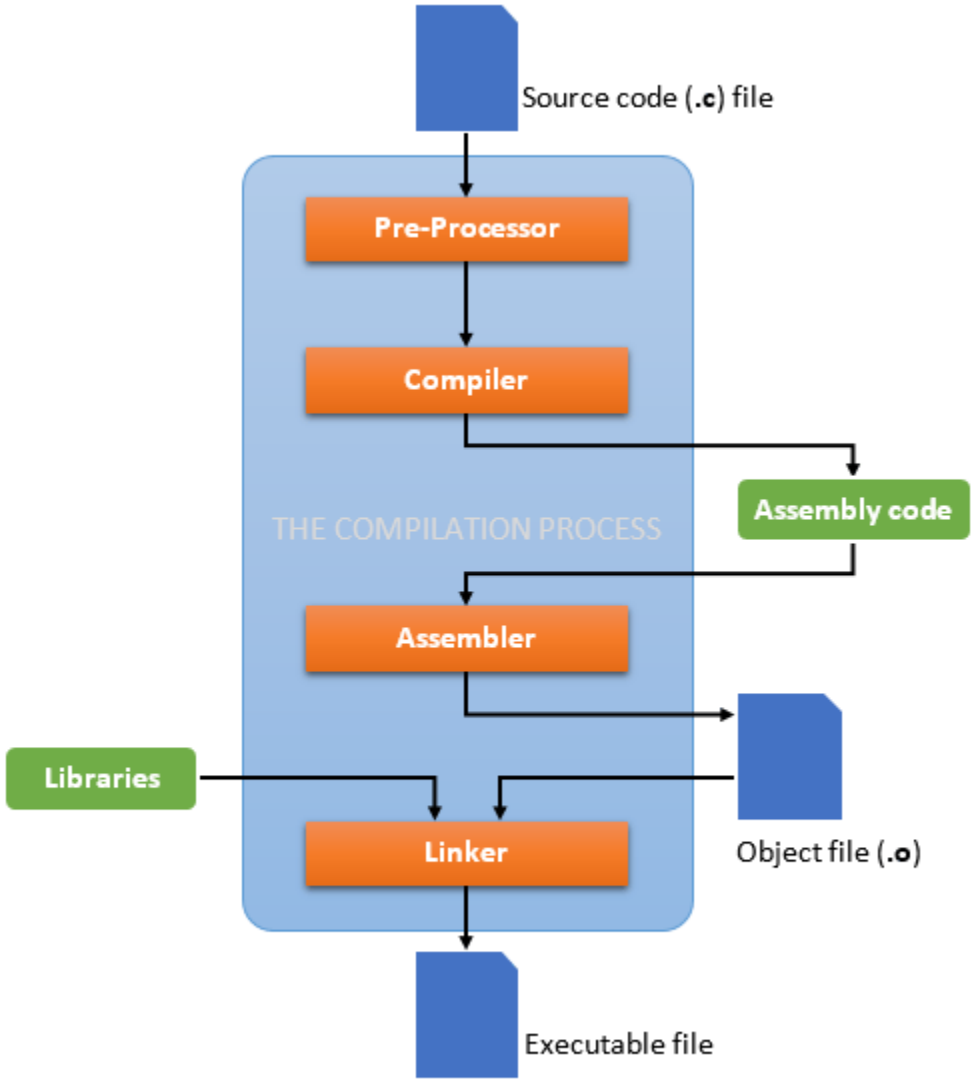
Reverse engineering is the processes of extracting knowledge or design information from anything man-made and re-producing it or re-producing anything based on the extracted information. The process often involves disassembling something (a mechanical device, electronic component, computer program, or biological, chemical, or organic matter) and analyzing its components and workings in detail.

Yeah Whatever……

- We will take either an already installed Android app or its APK file and will decompile it
- This will give us all of the code and resources that make this APK file
- And we will then:
  - Unzip the APK file
  - Decompile it
  - Make some changes to the source code
  - Recompile it
  - Sign it
  - Optimize it
  - Install it

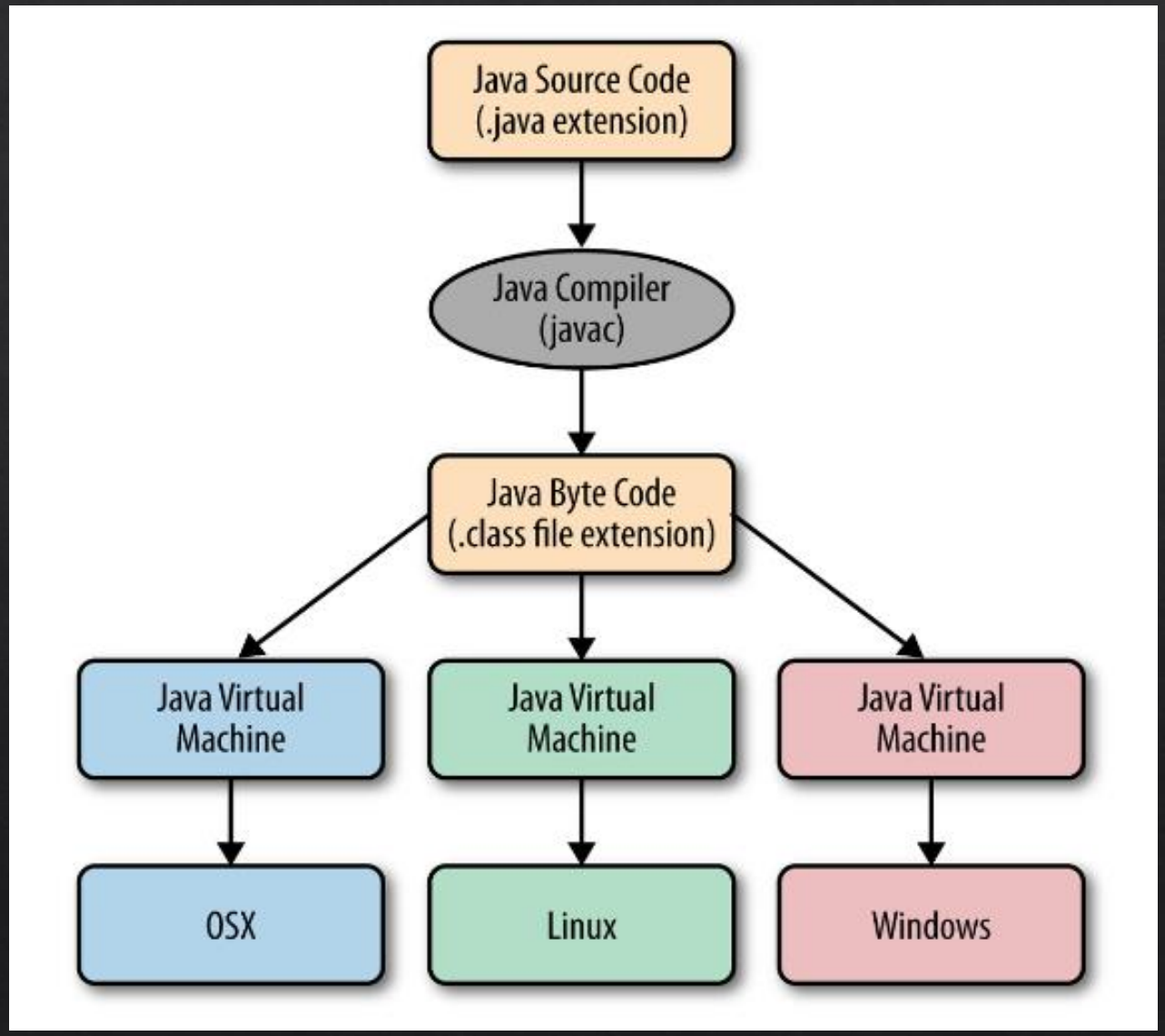
Android – Crash Course

C compilation process

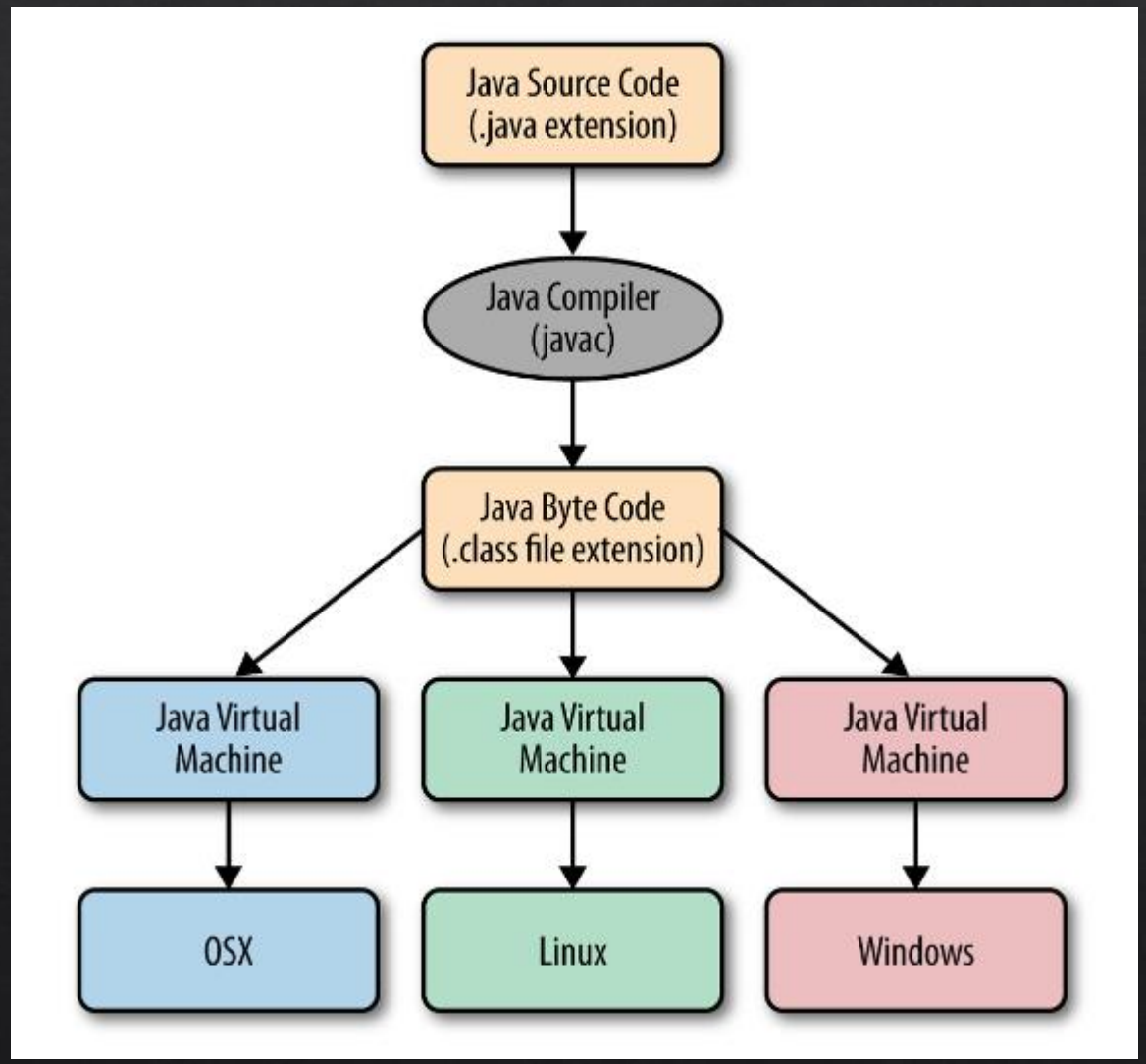


The C compilation process

Java compilation process



Java compilation process



Old Android compilation process