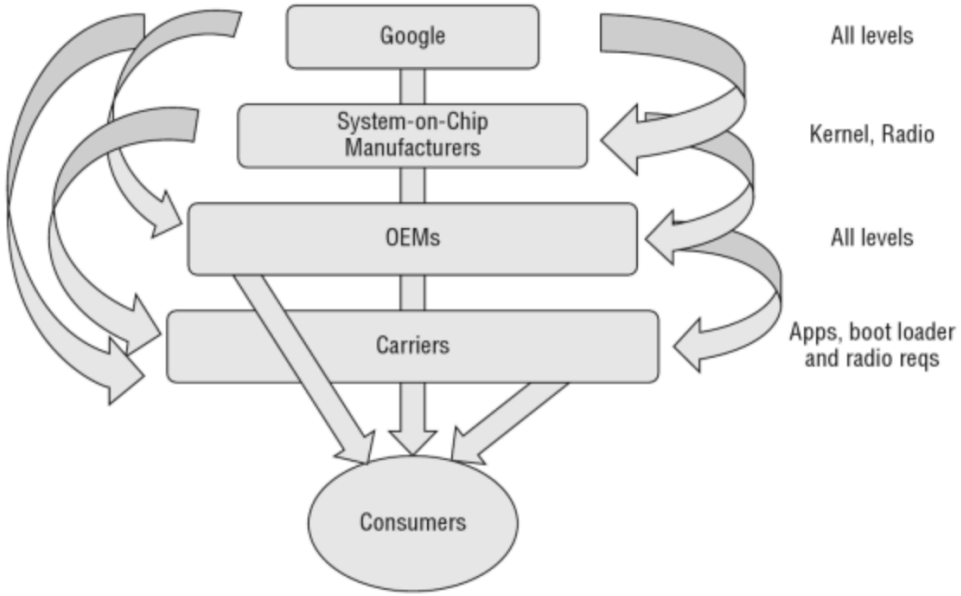
Pentesting Android Apps

Josh Wang

AOSP 101

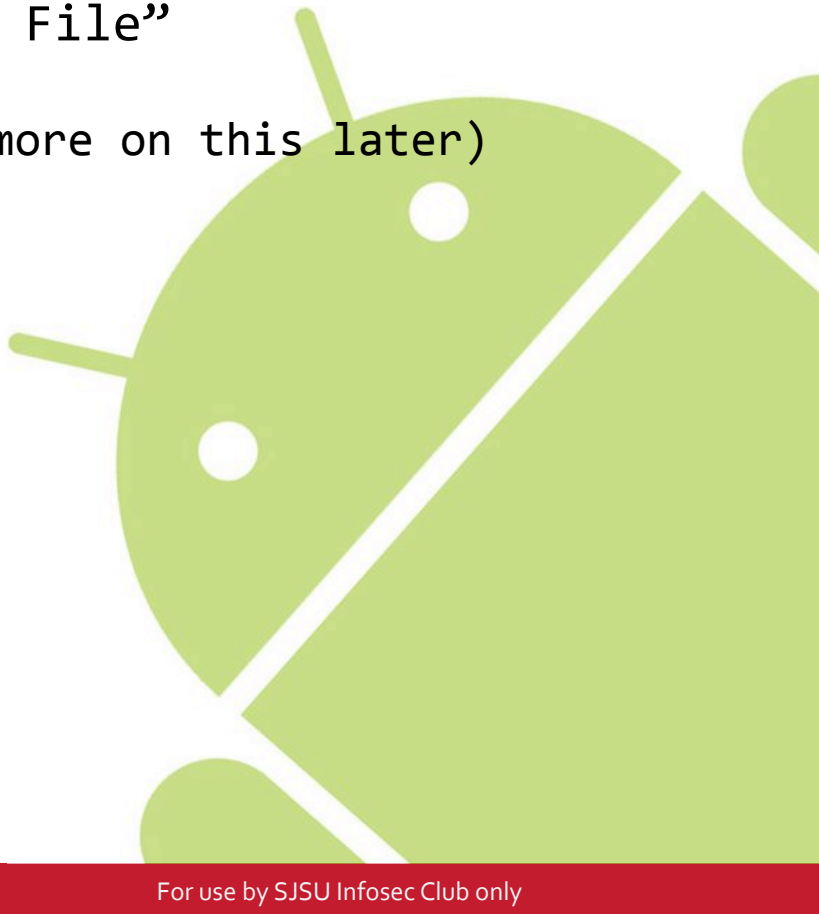


Android Ecosystem Relationships

source: Android Hacker's Handbook by Joshua Drake

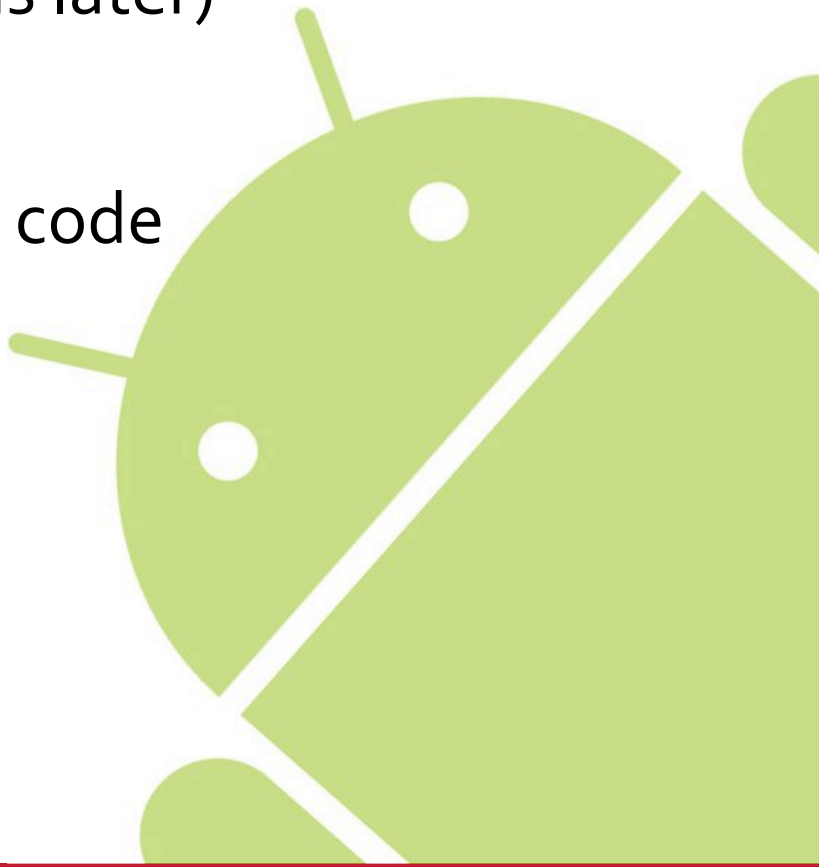
Keyterms

- Dalvik VM
  - Ea/process has its own instance
  - Executes .dex (Dalvik Executable) files
- AndroidManifest.xml / “Manifest File”
  - Configurations for each app
  - By default not human-readable (more on this later)
- Components
  - Intents
  - Activities
  - Services
  - Broadcast receivers
  - Content providers
  - Shared preferences



Android SDK, NDK

- SDK
  - Comes w/ADB (more on this later)
- NDK
  - Provides support for native code
  - Don’t rely on this!



ADB

- cmd line tool
- daemon on device
- server on host workstation

ADB Cheat Sheet

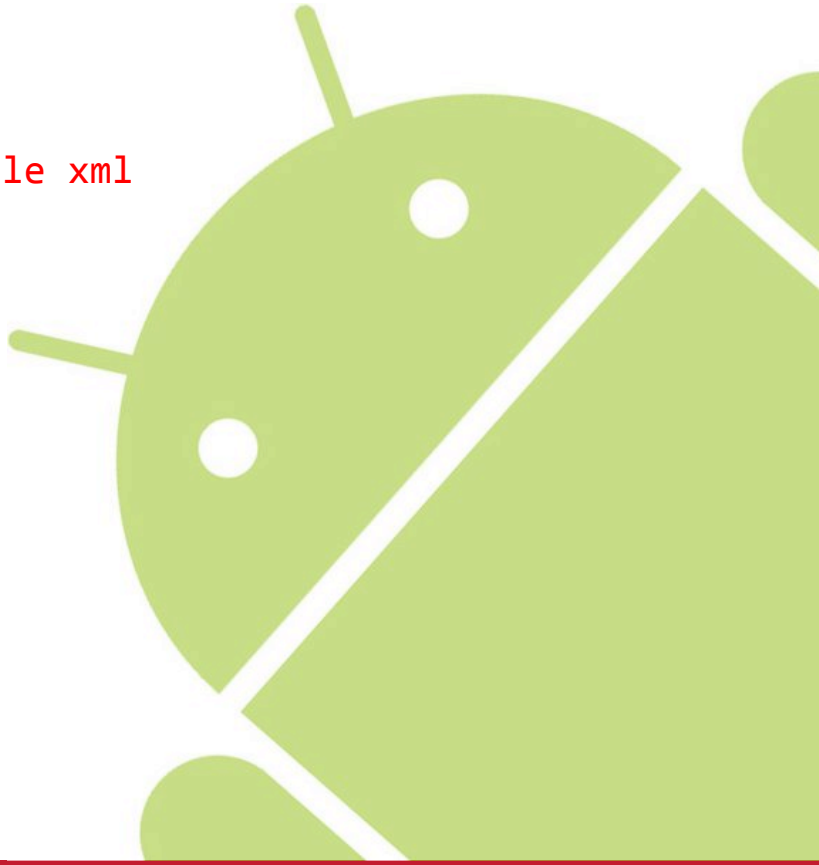
- adb devices
- adb shell
- adb pull <remote> <local>
- adb push <local> <remote>
- adb install <path_to_apk>
- adb logcat
- adb jdwp
  - lists open jdwp/debug sockets
- adb shell pm list packages –f
  - lists available packages and path to .apk's

Filesystem Directories

- /system/sbin ; /system/xbin
- /data/data
- /data/app
- /data/app-private

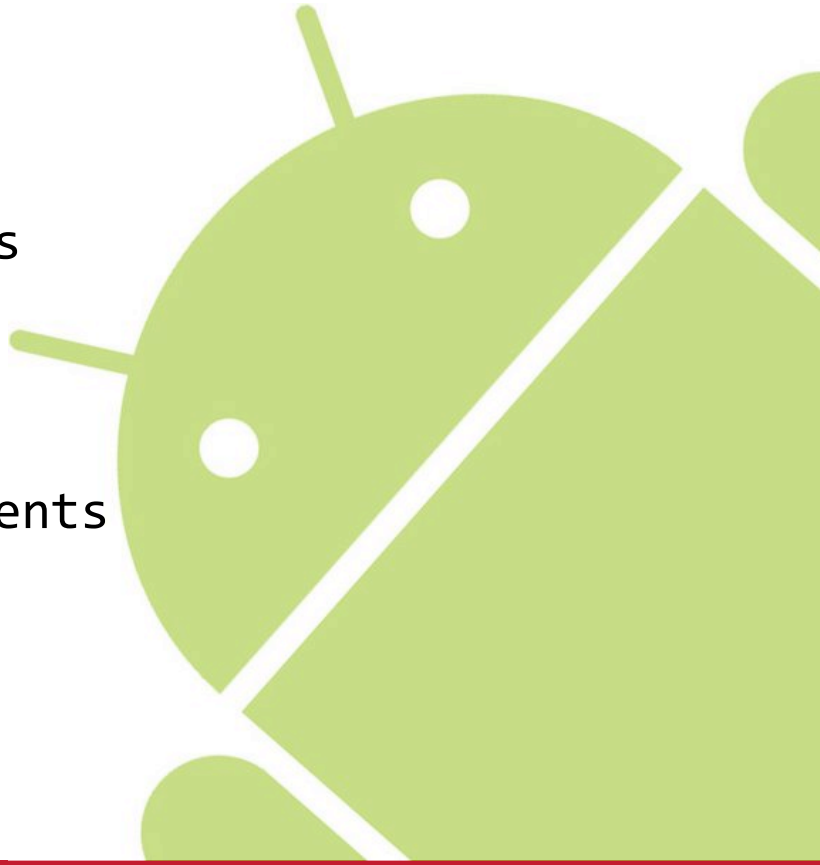
Essential Static Analysis Tools

- For extracting
  - APKtool
  - Unzip (yes, rly)
- For decompilation
  - APKtool
    - Convert binary xml to human-readable xml
    - Convert DEX bytecode to smali
  - Dex2Jar
    - Converts classes.dex to .jar file
  - JD-GUI
    - Decompiles java bytecode to approximate java source code
- For (re)building
  - APKtool
  - Jarsigner
  - Keytool



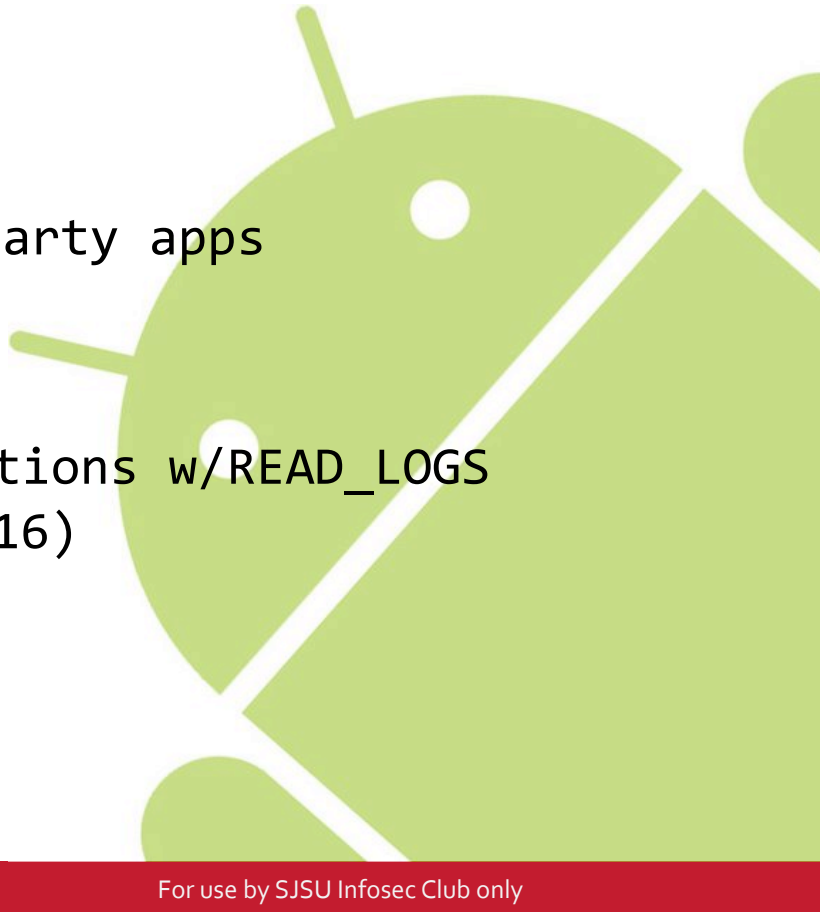
Essential Dynamic Analysis Tools

- logcat
  - logs available to apps w/READ_LOGS permission
- Burp Suite
  - best tool!
- Drozer
  - interacts w/ 4 IPC endpoints
  - enumerates IPC attack vectors
- JDB
  - kinda buggy
- GDB
  - analyzing native code components



Common Android Issues pt 1

- IPCs
  - Activities
  - Content Providers
    - Potential for SQLi
- Intent filter
  - Exposes applications to 3rd party apps
- Data storage
  - Sensitive data in logs
  - Logs are readable by applications w/READ_LOGS permissions (if < API level 16)



Common Android Issues pt 2

- Debug flag
  - *android:debuggable="true"*
  - Should be disabled in release builds
  - "@jdwp-control" Unix socket loop
  - Allows debuggable apps to connect to 3rd party Unix sockets opened by untrusted sources

http://resources.infosecinstitute.com/android-hacking-security-part-6-exploiting-debuggable-android-applications/

Common Android Issues pt 3

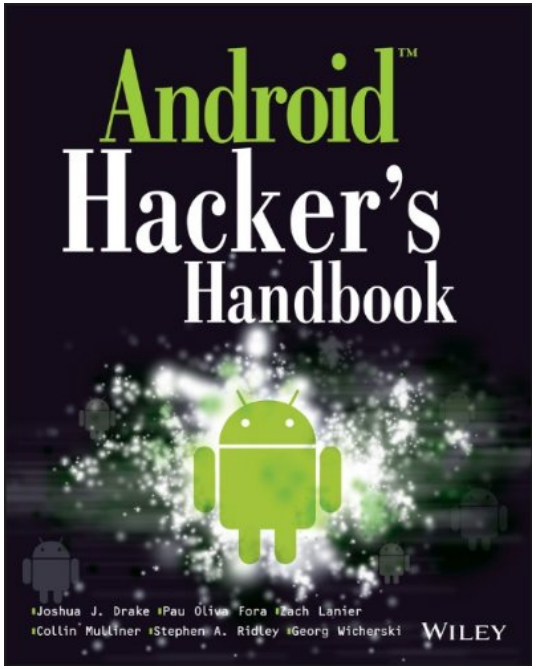
- WebView
  - setJavaScriptEnabled(true);
  - addJavascriptInterface();
  - Remote Code Execution!
    - POC: https://github.com/jduck/VulnWebView/

https://labs.mwrinfosecurity.com/blog/2013/09/24/webview-addjavascriptinterface-remote-code-execution/

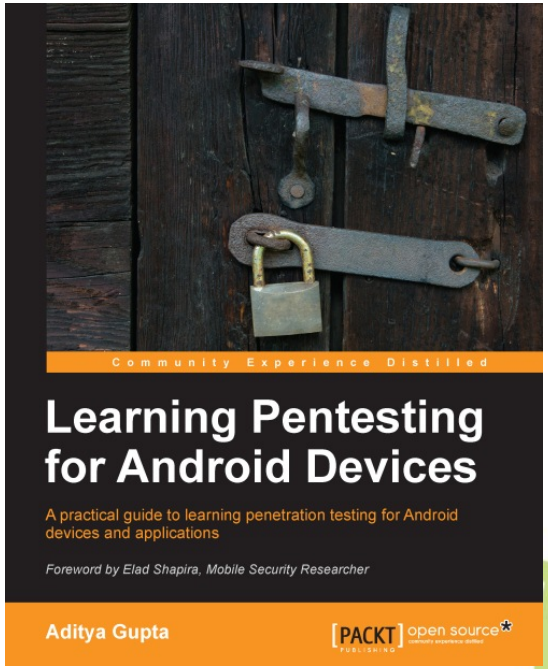
Code Signing

- Pervasive but is it enough?

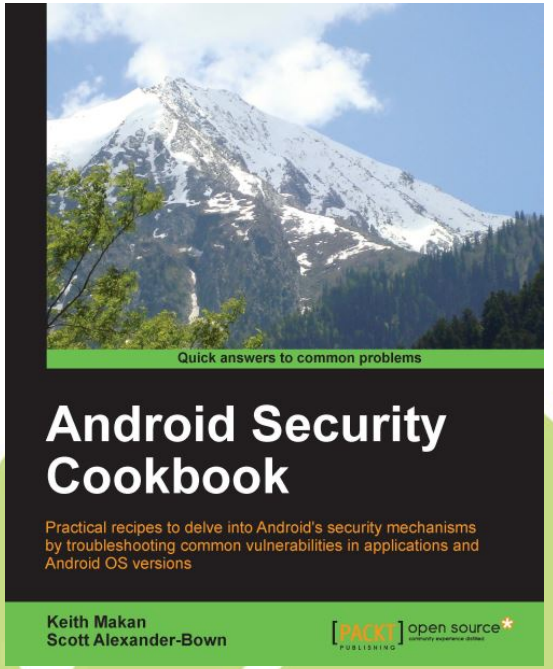
Books



Android Hacker's Handbook
by Joshua Drake



Learning Pentesting for Android Devices
by Aditya Gupta



Android Security Cookbook
by Keith Makan & Scott Alexander-Brown

Demo Time!