Bypassing Android Binary Protections

Julian Berton?

- Application Security tester
- OWASP Melbourne chapter lead
- Was a developer

Contact

- meetup.com/Application-Security-OWASP-Melbourne/
- @JulianBerton (Twitter - not very active)

Why are you here and not at the bar?

- Android, a quick intro?
- What are binary protections?
- Why do we need to bypass them?
- The different types of protections.
- How we can bypass them?
- Lots of bypass demos!

Android

- Mostly open source mobile operating system
- Android Open Source Project (AOSP)
-

2008 ---------- 2010

Cupcake
Android 1.5

Donut
Android 1.6

Eclair
Android 2.0/2.1

Froyo
Android 2.2.x

Gingerbread
Android 2.3.x

2011 ---------- 2015

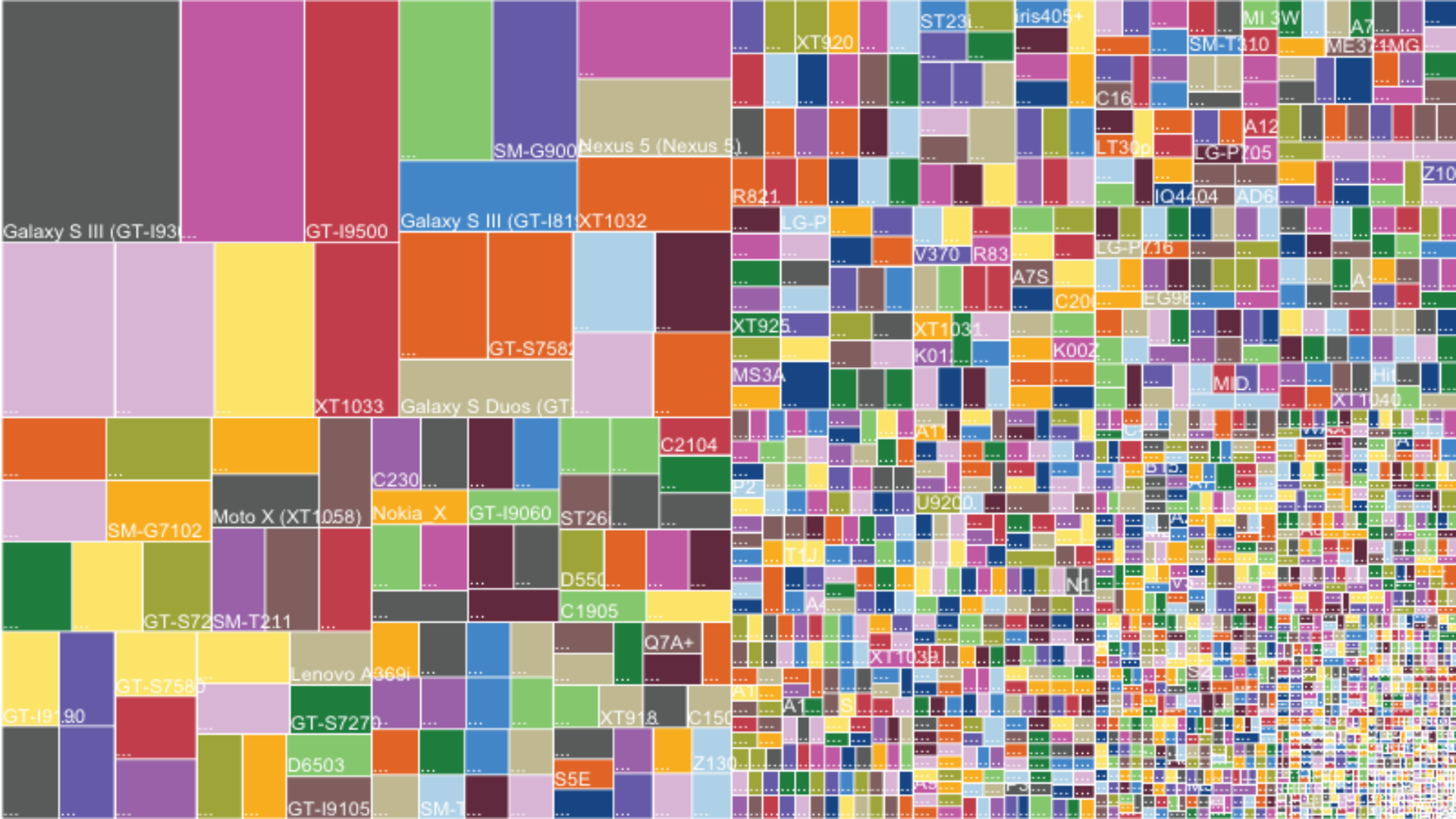
Honeycomb
Android 3.x

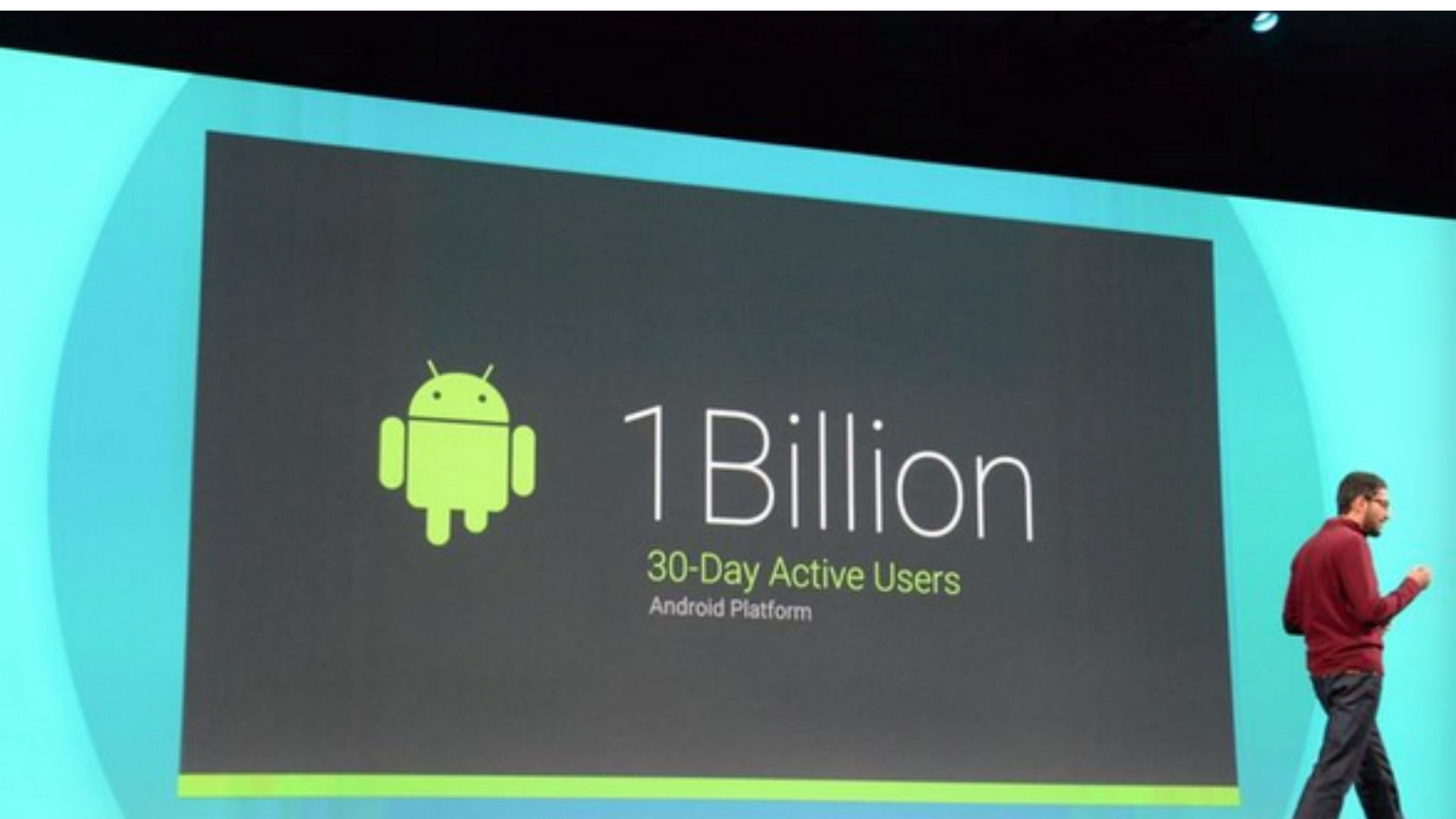
Ice Cream Sandwich
Android 4.0.x

Jelly Bean
Android 4.1.x

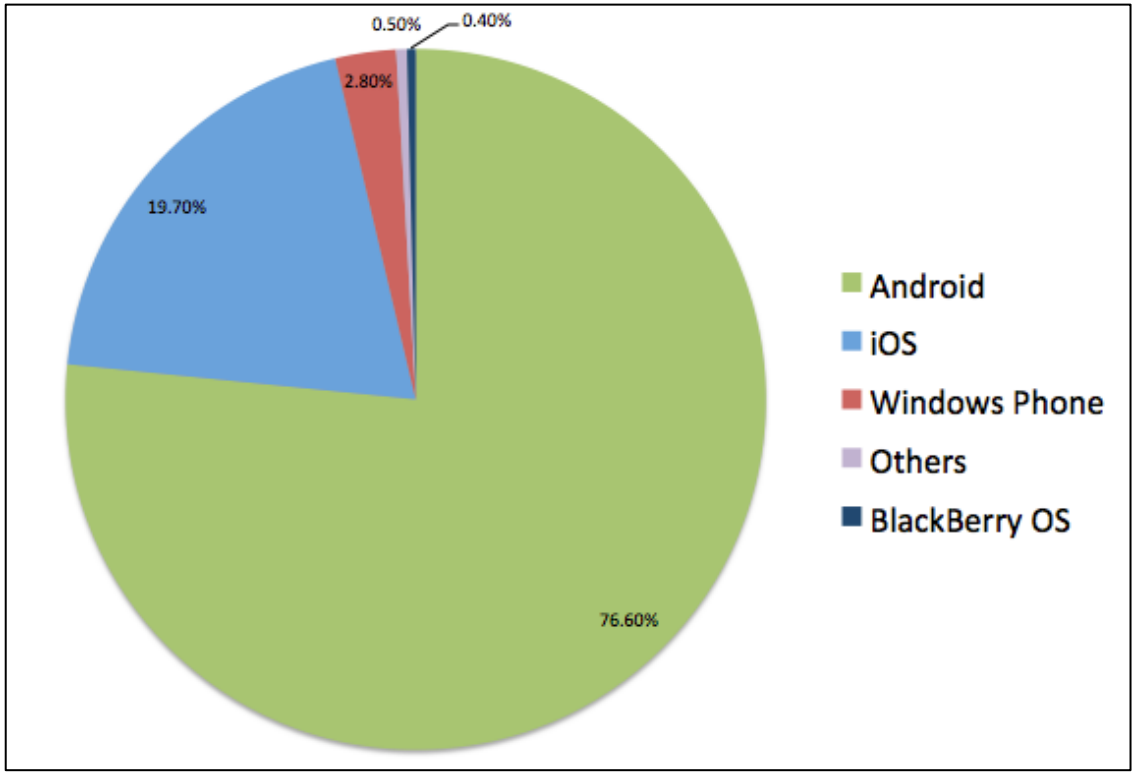
KitKat
Android 4.4.x

Lollipop
Android 5.0


Galaxy S III (GT-I93
GT-I9500
SM-G900
Nexus 5 (Nexus 5)
Galaxy S III (GT-I81
XT1032
XT1033
GT-S758
Galaxy S Duos (GT
C2104
C230
Nokia X
GT-I9060
ST26
SM-G7102
Moto X (XT1058)
D550
GT-S72
SM-T211
C1905
Q7A+
Lenovo A369i
GT-S758
GT-I9
90
GT-S727
XT918
C150
D6503
S5E
Z130
GT-I9105
XT920
ST23i
iris405+
MI 3W
SM-T
10
A7
ME3
MG
C16
A12
LT30
LG-P
705
Z10
R821
IQ44
04
AD6
LG-P
V370
R83
A7S
C20
XT925
XT103
K01
K00
MS3A
M
D.
XT1040
U920
T1J
N1
XT103
A1
S


1 Billion
30-Day Active Users
Android Platform

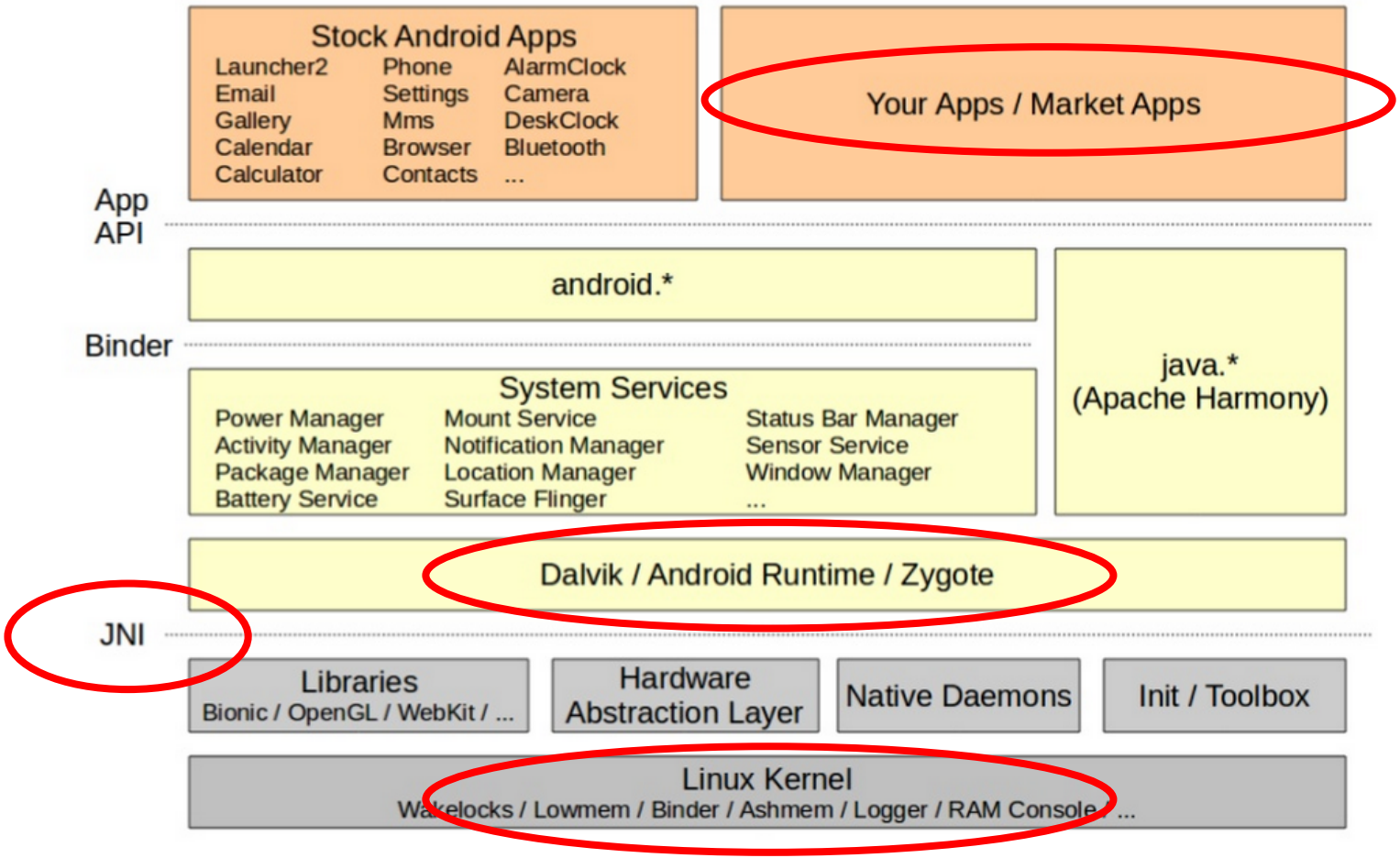
Smartphone OS Market Share



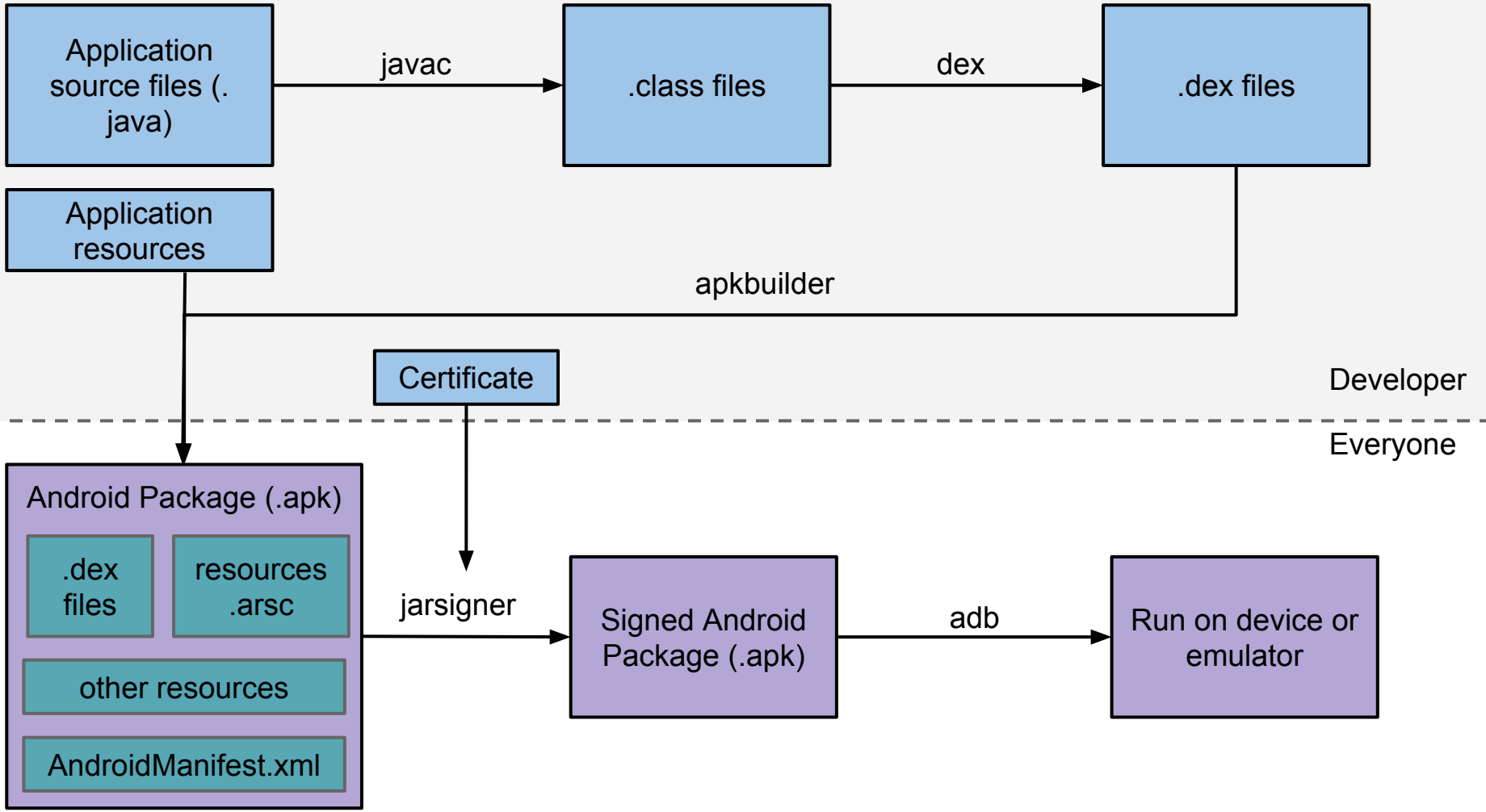
=

Source: IDC, 2014 Q4

Android System Architecture

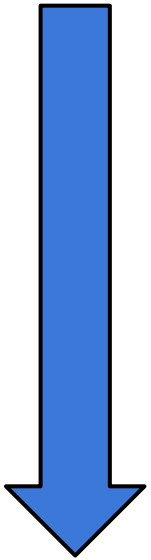

Stock Android Apps
Launcher2
Email
Gallery
Calendar
Calculator
Phone
Settings
Mms
Browser
Contacts
AlarmClock
Camera
DeskClock
Bluetooth
...
Your Apps / Market Apps
App API
android.*
java.*
(Apache Harmony)
Binder
System Services
Power Manager
Activity Manager
Package Manager
Battery Service
Mount Service
Notification Manager
Location Manager
Surface Flinger
Status Bar Manager
Sensor Service
Window Manager
...
Dalvik / Android Runtime / Zygote
JNI
Libraries
Bionic / OpenGL / WebKit / ...
Hardware Abstraction Layer
Native Daemons
Init / Toolbox
Linux Kernel
Wakelocks / Lowmem / Binder / Ashmem / Logger / RAM Console / ...

Android Application Build Process


Application source files (. java)
javac
.class files
dex
.dex files
Application resources
apkbuilder
Certificate
Developer
Everyone
Android Package (.apk)
.dex files
resources .arsc
other resources
AndroidManifest.xml
jarsigner
Signed Android Package (.apk)
adb
Run on device or emulator

Binary What?

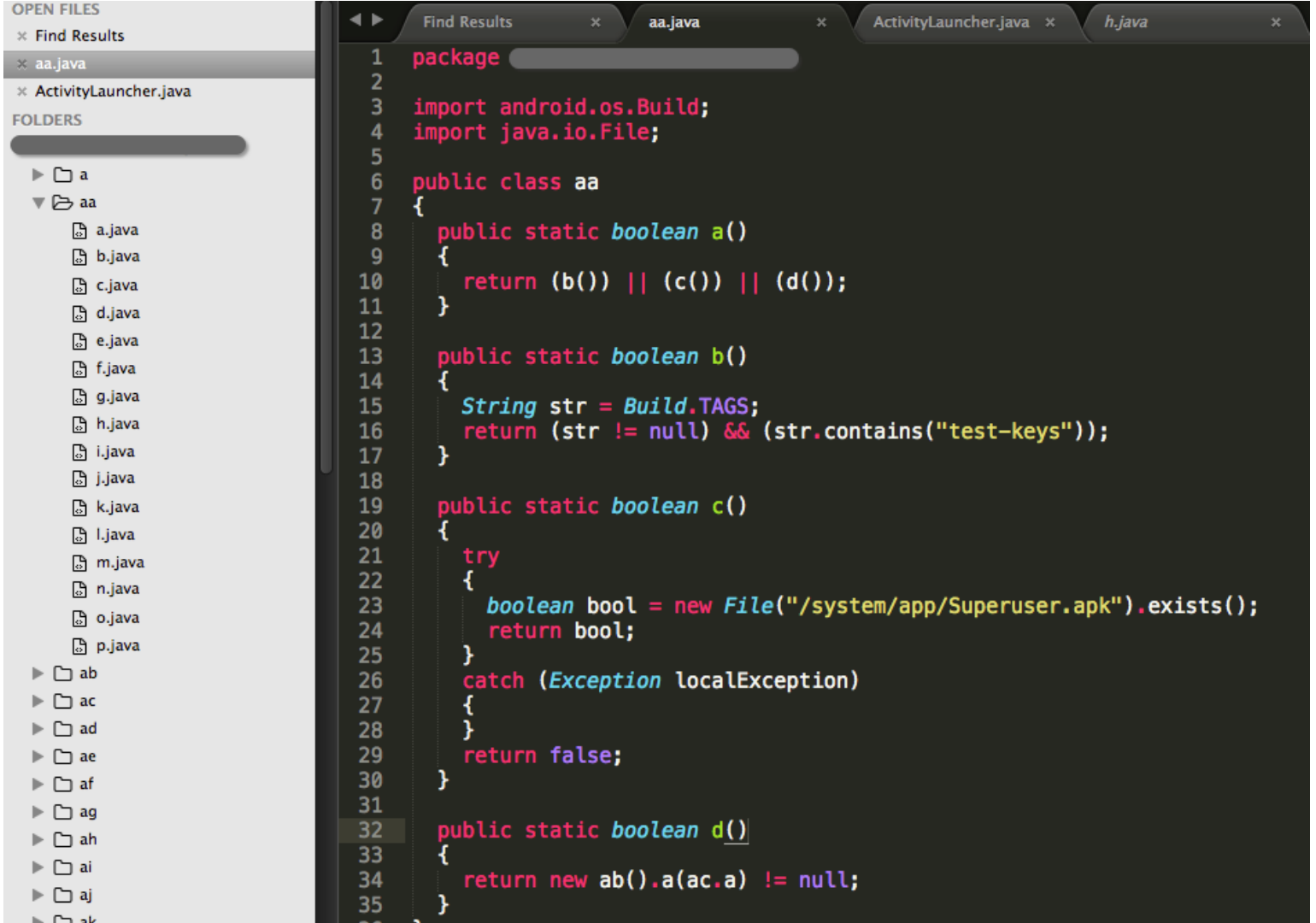
1. Code obfuscation
2. SSL pinning
3. Root detection
4. Debugger checks
5.
6. Others



Ordered by popularity

Source: me

```
$ openssl x509 -in freesoft-certificate.pem -noout -text
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 7829 (0x1e95)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/emailAddress=server-certs@thawte.com
        Validity
            Not Before: Jul  9 16:04:02 1998 GMT
            Not After : Jul  9 16:04:02 1999 GMT
        Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                 OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                    33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                    66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                    70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                    16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                    c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                    8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                    d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                    e8:35:1c:9e:27:52:7e:41:8f
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
```

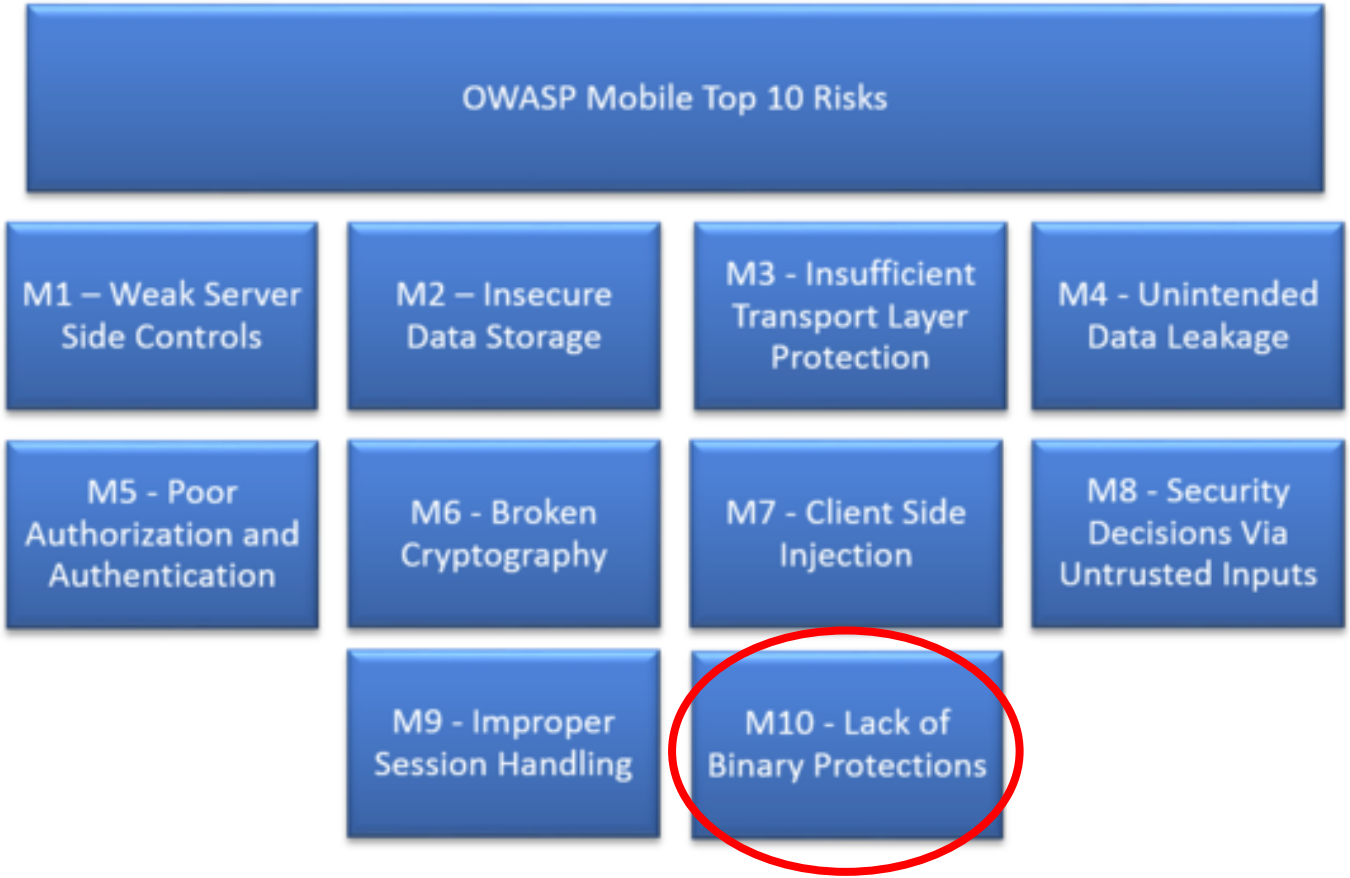

OPEN FILES
Find Results
aa.java
ActivityLauncher.java
FOLDERS
a
aa
a.java
b.java
c.java
d.java
e.java
f.java
g.java
h.java
i.java
j.java
k.java
l.java
m.java
n.java
o.java
p.java
ab
ac
ad
ae
af
ag
ah
ai
aj
Find Results
aa.java
ActivityLauncher.java
h.java
1 package
2
3 import android.os.Build;
4 import java.io.File;
5
6 public class aa
7 {
8 public static boolean a()
9 {
10 return (b()) || (c()) || (d());
11 }
12
13 public static boolean b()
14 {
15 String str = Build.TAGS;
16 return (str != null) && (str.contains("test-keys"));
17 }
18
19 public static boolean c()
20 {
21 try
22 {
23 boolean bool = new File("/system/app/Superuser.apk").exists();
24 return bool;
25 }
26 catch (Exception localException)
27 {
28 }
29 return false;
30 }
31
32 public static boolean d()
33 {
34 return new ab().a(ac.a) != null;
35 }

Got Rooted?

```
201   protected void onCreate(Bundle paramBundle)
202   {
203     super.onCreate(paramBundle);
204     setContentView(2130903072);
205     if (aa.a())
206     {
207       com.fake.blah.d.d(this, "Device Rooted");
208       finish();
209       return;
210     }
211     g.a(this, getString(2131296433));
212     if ((getIntent() != null) && (getIntent().hasExtra(WAHCKon.a)))
213       getSharedPreferences(getString(2131296432), 0).edit().putBoolean(WAHCKon.a, true).apply();
214     m();
215   }
```

Why Do I Need Them - Developers\Businesses?

- Intellectual property theft
- Brand damage
- Reduce number of attacks
- Because OWASP says...

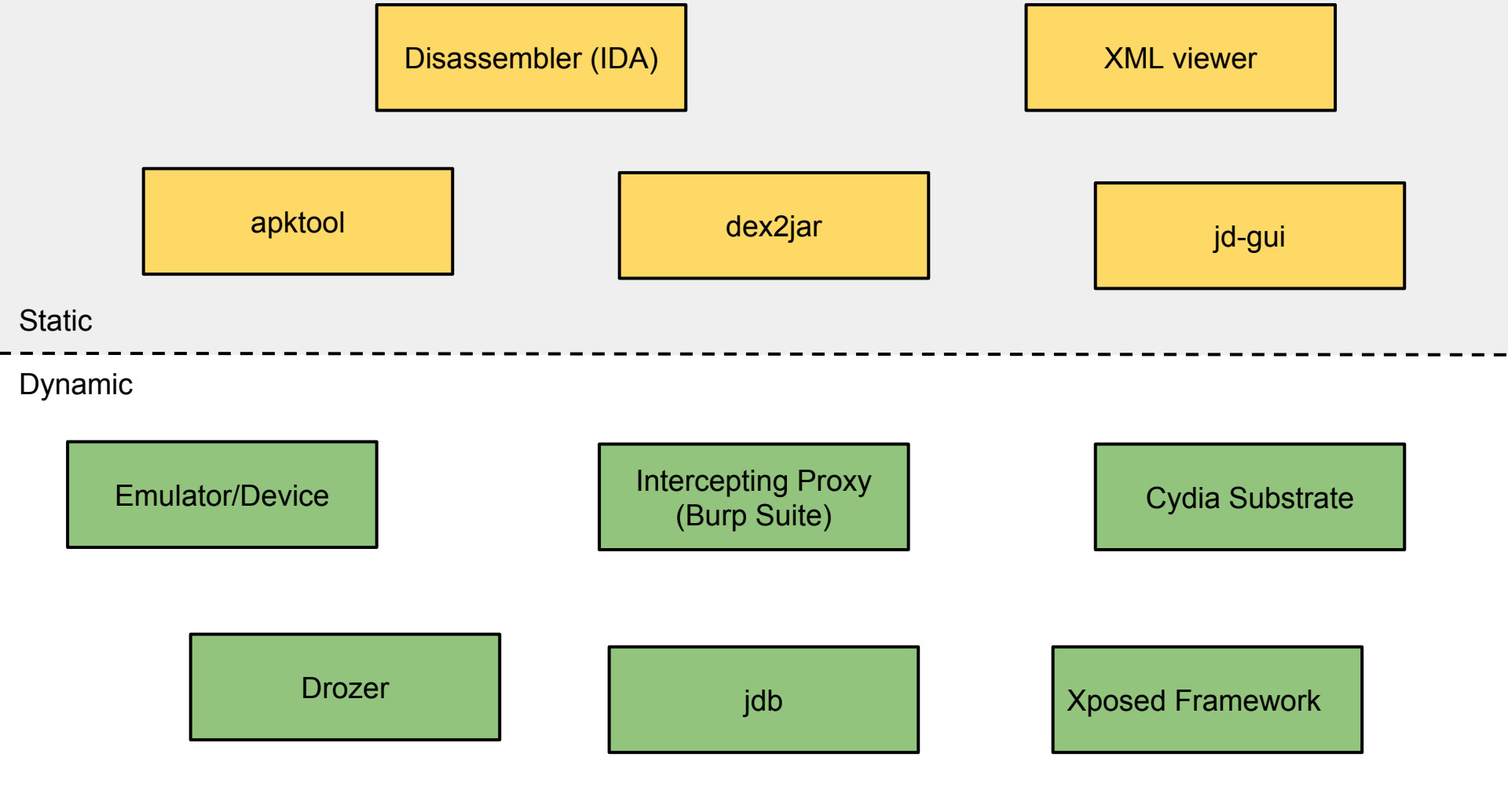

OWASP Mobile Top 10 Risks
M1 – Weak Server Side Controls
M2 – Insecure Data Storage
M3 - Insufficient Transport Layer Protection
M4 - Unintended Data Leakage
M5 - Poor Authorization and Authentication
M6 - Broken Cryptography
M7 - Client Side Injection
M8 - Security Decisions Via Untrusted Inputs
M9 - Improper Session Handling
M10 - Lack of Binary Protections

Why Do We Care - Pen testers?

- Need to bypass the protections to perform analysis and find vulnerabilities.

Environment Setup

- SDK tools - includes Android Developer Bridge (adb)
- Android Emulator or a rooted Android device
- Apktool - decodes and rebuilds apk files
- dex2jar - as the name suggests
- jd-gui - takes jar file and converts to Java source code
- Cydia Substrate - runtime manipulation/hooking
- Xposed Framework - runtime manipulation/hooking


Disassembler (IDA)
XML viewer
apktool
dex2jar
jd-gui
Static
Dynamic
Emulator/Device
Intercepting Proxy
(Burp Suite)
Cydia Substrate
Drozer
jdb
Xposed Framework

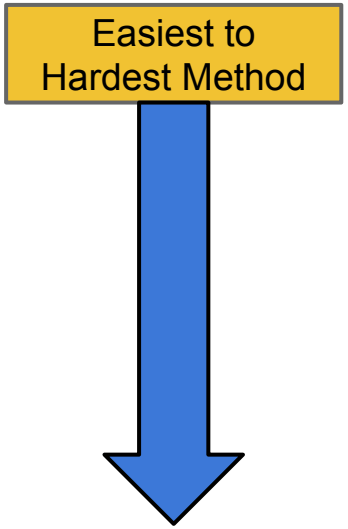
Bypassing Root Detection And SSL Pinning

Bypass Methods

1. Install apps that try to hide root

2. Install Cydia Substrate or Xposed and write a module

3. Modify the smali and build the app



Demo!!

More Info?

1. Root Detection Bypass - https://bertonjulian.github.io/2015/01/30/root-detection-bypass.html

2. Android SSL Pinning Bypass - http://opentechnotes.blogspot.com.au/2015/01/intercept-all-http-ssl-android-traffic.html

References

- Android System Arcitecture - http://anatomyofandroid.com/2013/10/15/zygote/
- Android build process - https://developer.android.com/sdk/installing/studio-build.html
- Dalvik vs ART - https://source.android.com/devices/tech/dalvik/index.html
- SSL Pinning - https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning
- SSL Pinning Google - https://developer.android.com/training/articles/security-ssl.html
- Anti-reverse engineering - https://bluebox.com/wp-content/uploads/2013/05/AndroidREnDefenses201305.pdf
- OWASP Mobile Top 10 - https://www.owasp.org/index.php/Mobile_Top_10_2014-M10

References - Tools

- Xposed Framework - http://repo.xposed.info/
- Genymotion - https://www.genymotion.com/
- apktool - https://ibotpeaches.github.io/Apktool/
- Cydia Substrate - http://www.cydiasubstrate.com/
- Android SDK - https://developer.android.com/sdk/index.html#Other
- dex2jar - https://github.com/pxb1988/dex2jar
- jd-gui - http://jd.benow.ca/
- jdb - https://docs.oracle.com/javase/7/docs/technotes/tools/windows/jdb.html

References - Images

- http://www.firstpost.com/wp-content/uploads/2013/09/01_Android-all-versions.jpg
- http://opensignal.com/reports/2014/android-fragmentation/
- https://www.theverge.com/2014/6/25/5841924/google-android-users-1-billion-stats
- http://jaredrummler.com/2014/11/09/lollipop-land/
- http://www.slideshare.net/opersys/inside-androids-ui