

Android Root Detection Evasion

Roberto Castellotti

Supervised by: Prof. Giovanni Lagorio

Università di Genova

2022

fundamentals: Android



Figure: <https://source.android.com/devices/architecture>

fundamentals: java to bytecode and back

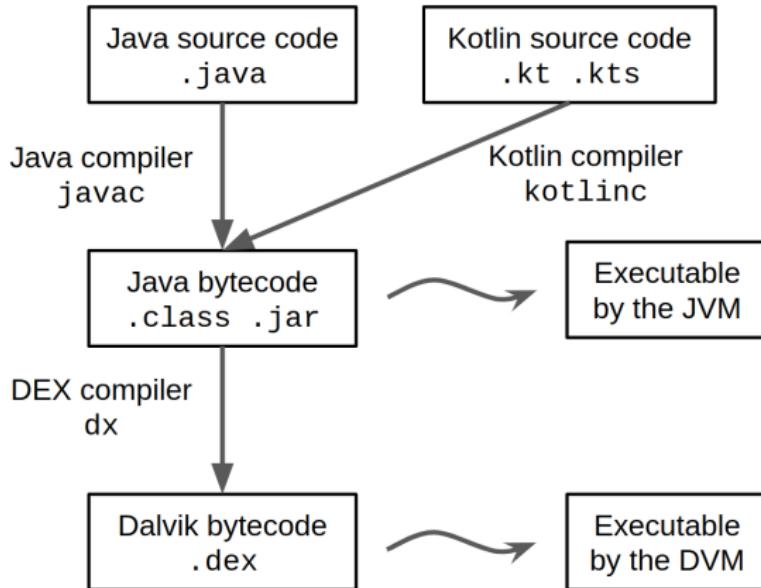


Figure: MOBISec 2020 - 10 - Native Code

.dex and .smali

- up until android 4.4 "KitKat" Dalvik was integral part of software stack
- dx is used to convert Java .class to .dex format executable by the DVM
- from android 5.0 "Lollipop" ART is the only included runtime, uses same bytecode and .dex files
- [JesusFreke/smali](#): assembler/disassembler for the dex format used by dalvik, we obtain smali code when decompiling with apktool

sample smali code

```
.method private static checkRootMethod1()Z
    .registers 2
    .line 1
    sget-object v0, Landroid/os/Build;->TAGS:Ljava/lang/String;
    if-eqz v0, :cond_e
    const-string v1, "test-keys"
    .line 2
    invoke-virtual {v0, v1}, Ljava/lang/String;->contains(Ljava/lang/CharSequence;)Z
    move-result v0
    if-eqz v0, :cond_e
    const/4 v0, 0x1
    goto :goto_f
    :cond_e
    const/4 v0, 0x0
    :goto_f
    return v0
.end method
```

root detection: how

a

root detection: how

- check for root management apps (com.topjohnwu.magisk)

```
import android.content.pm.PackageManager;
import android.content.Context;
private final Context mContext;
PackageManager pm = mContext.getPackageManager();
pm.getPackageInfo(packageName, 0);
```

- check root cloaking appps

```
(com.devadvance.rootcloak, de.robv.android.xposed.installer)
```

- check for dangerous applications (com.dimonvideo.luckypatcher)

- check for binaries (busybox, su)

```
File f = new File(path, filename);
boolean fileExists = f.exists();
```

- check if some paths are writable (/system, /sbin, /etc)

```
InputStream inputStream = Runtime.getRuntime().exec("mount")
```

patch-and-reinstall

- adb pull /data/com/app/com.package.name app.apk
- apktool d app.apk -output app
- patch
- apktool b app -output rebuilt-app.apk
- zipalign -f -p 4 rebuilt-app.apk aligned-rebuilt-app.apk
- apksigner sign --ks /key.jks aligned-rebuilt-app.apk
- adb install aligned-rebuilt-app.apk
- this approach does not require the android device to be rooted

patch-and-reinstall: an example

The patching process is usually a matter of finding the methods performing root detection and patching them, here is an example from a popular financial services company's application:

```
Author: rcastellotti <me@rcastellotti.dev> 2022-06-29 01:17:32
Committer: rcastellotti <me@rcastellotti.dev> 2022-06-29 01:17:32
Parent: 4e6c812897a3d9e1187e9fafd77619b8f2b0540a (decompiled)
Child: 20844736e60bf9879250e4d4ed48af41b143 (added [REDACTED] patch)
Branches: main, remotes/origin/main
Follows:
Precedes:

i cant really believe this is the patch

[REDACTED] /smali_classes2/com/[REDACTED] /util/WuRootUtil.smali
index 6460600e0..866aaef619 100644
@@ -329,7 +329,7 @@
 
 :cond_1
 :goto_0
- const/4 v0, 0x1
+ const/4 v0, 0x0

 :goto_1
 return v0
```

Figure: patching `.method public static isDeviceRooted()Z`

frida: a dynamic toolkit

- provides ability to inject scripts into black box processes.
- portable (Windows, macOS, GNU/Linux, iOS, Android)
- **injected mode:** frida-server: frida-core over TCP
- frida-core: a layer that packages up GumJS into a shared library that it injects into existing software, and provides a two-way communication channel for talking to your scripts.
- **on device:** ./frida-server-15.1.27-android-arm64
- **on computer:** frida -U -l script.js -f com.package.name
- this approach could be better since it allows to patch applications without losing original package signature

frida: script.js

```
Java.perform(function () {
    var PackageManager = Java.use("android.app.ApplicationPackageManager");
    var NativeFile = Java.use("java.io.File");
    var Runtime = Java.use("java.lang.Runtime");

    PackageManager.getPackageInfo.overload(
        "java.lang.String",
        "int"
    ).implementation = function (pname, flags) {
        send("Bypass root check for package: " + pname);
        pname = "set.package.name.to.a.fake.one.so.we.can.bypass.it";
    }
    return this.getPackageInfo
        .overload("java.lang.String", "int")
        .call(this, pname, flags);
};

NativeFile.exists.implementation = function () {
    var name = NativeFile.getName.call(this);
    send("Bypass return value for binary: " + name);
    return false;
};
});
```

com.revolut.revolut (fintech)

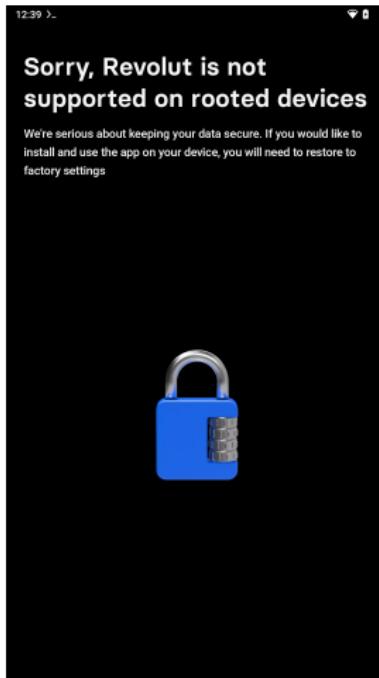


Figure: original apk

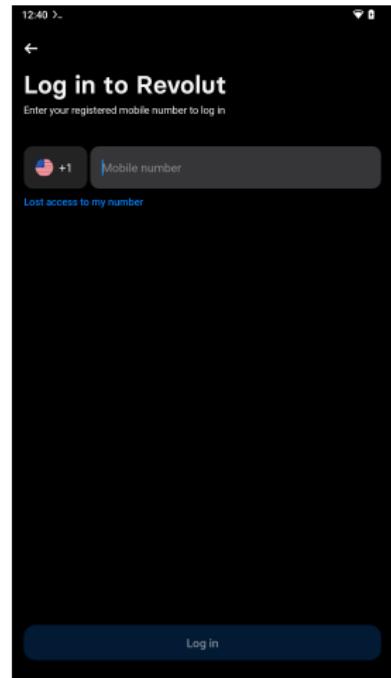


Figure: patched

com.scottyab.rootbeer.sample

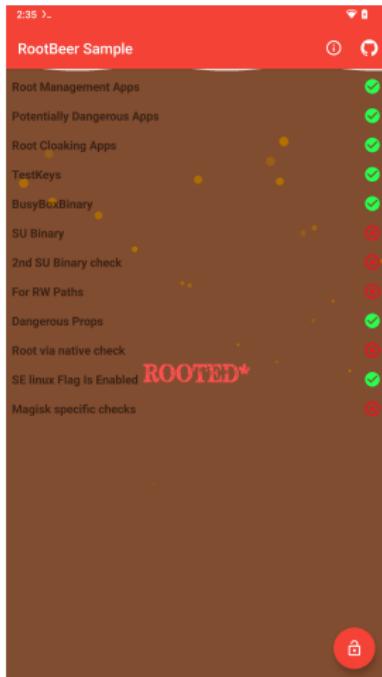


Figure: original apk

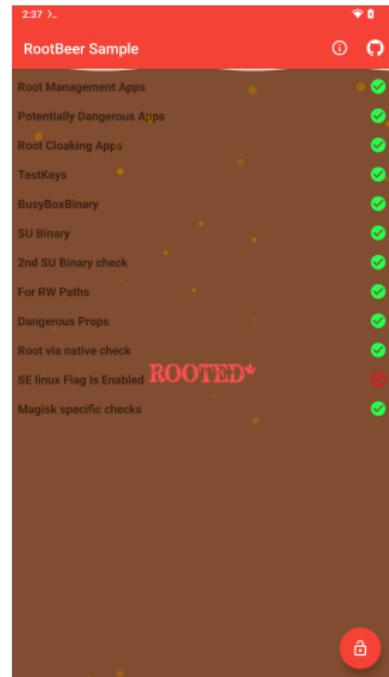


Figure: patched

a popular financial services company's application

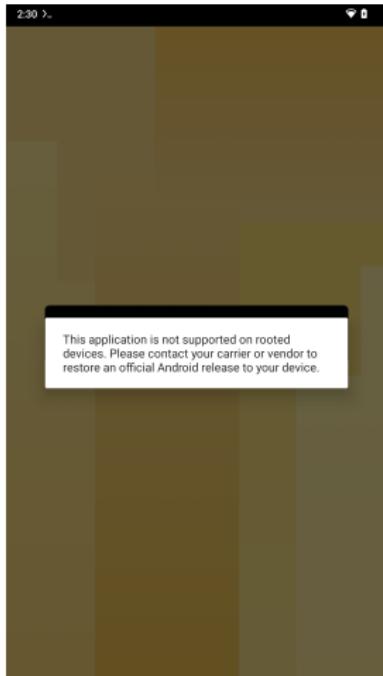


Figure: original apk

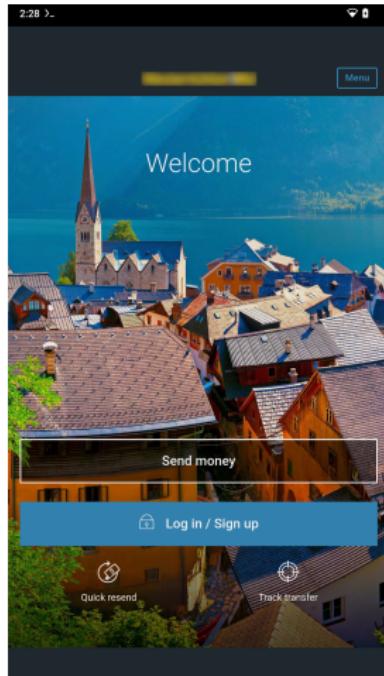


Figure: patched

tools and sources

- [Android Studio](#)
- [iBotPeaches/Apktool](#): A tool for reverse engineering Android apk files
- [skylot/jadx](#): Dex to Java decompiler
- [scottyab/rootbeer](#): root checking Android library and sample app
- <https://en.wikipedia.org/wiki/Dalvik>
- [Dalvik Bytecode](#)
- [Anroid Runtime](#)
- <https://developer.android.com/guide/components/fundamentals>