# Deal with Reverse Engineering

@catvinhquang

Sep 20th 2019

### Agenda

- ProGuard / R8: Obfuscate code
- II. Signature recognition
- III. Hide view IDs (like Facebook / Messenger)
- IV. Extra tips

Demo: https://github.com/catvinhquang/deal-with-reverse-engineering



### I. ProGuard / R8: How it works?

Android Gradle plugin 3.4.0+ no longer uses ProGuard to perform compile-time code optimization. Instead, the plugin works with the R8 compiler to handle the following compile-time tasks:

- Code shrinking: removes unused classes, fields, methods, and attributes
- Resource shrinking: removes unused resources
- Obfuscation: shortens the name of classes and members
- Optimization: inspects and rewrites your code

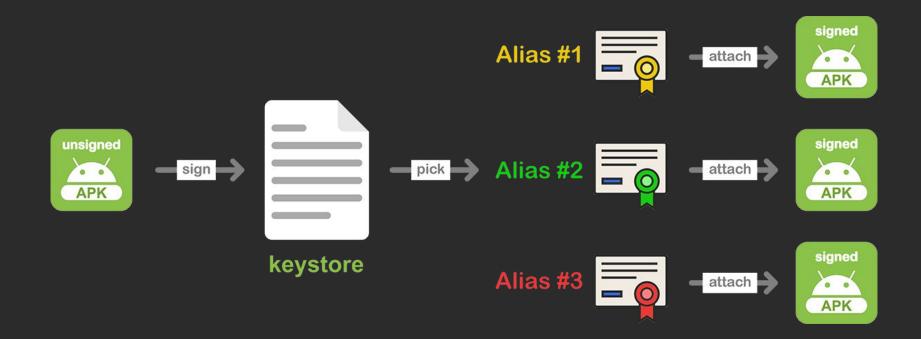


### I. ProGuard / R8: Setup

```
android {
   buildTypes ·
        release {
            // Enables code shrinking, obfuscation, and optimization for only
            // your project's release build type.
           minifyEnabled true
            // Android Gradle plugin.
            shrinkResources true
            // Includes the default ProGuard rules files that are packaged with
            // the Android Gradle plugin. To learn more, go to the section about
            // R8 configuration files.
            proguardFiles getDefaultProguardFile(
                     proguard-android-optimize.txt'),
                    'proquard-rules.pro'
```

build.gradle in app module

### II. Signature recognition: Signing process



### II. Signature recognition: Detect APK changes

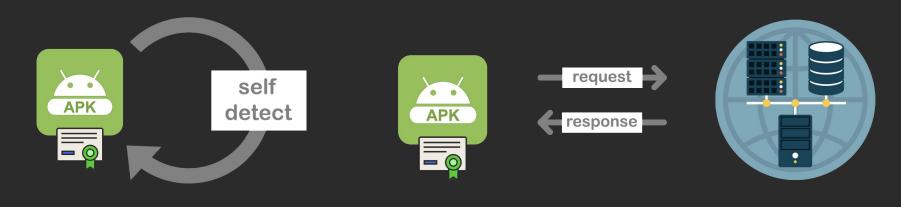


Figure 1. Local check

Figure 2. Server check

### III. Hide view IDs: Why?

### Tools to find view IDs:

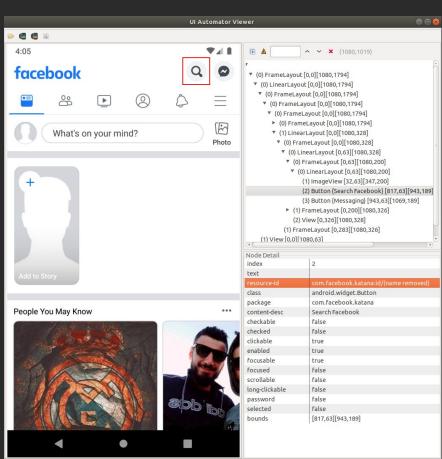
- androidsdk / tools / bin / uiautomatorviewer
- androidsdk / tools / platform-tools / adb shell dumpsys activity top

### The effect of hiding view IDs:

- Positive: Determining the point of attack will be harder
- Negative: Automated testing will be harder

#### uiautomatorviewer

## adb shell dumpsys activity top



```
quang@Quang-PC: ~
File Edit View Search Terminal Help
                         X.1UJ{c9ead89 VFED..... .....I. 0,0-1080,1794 #102000a android:id/list}
                            com.facebook.litho.ComponentHost{c66552f VFED..C.. ...... 969,9-1064,104}
                            com.facebook.litho.ComponentHost{6e0c73c VFED..C.. ...... 969,16-1064,111}
                            com.facebook.litho.ComponentHost{ed14cc5 VFED..C.. ...... 969.9-1064.104}
                            com.facebook.litho.ComponentHost{9dfe61a VFED..C....... 969.9-1064.104}
                            com.facebook.litho.ComponentHost{e8d154b VFED..C.. ...... 969.9-1064.104}
                            com.facebook.litho.ComponentHost{1911b28 VFED..C.. ...... 969,12-1064,107}
                            com.facebook.litho.ComponentHost{9fef041 VFED..C.. ...... 969,12-1064,107}
                         X.1Ts{20649e6 G.ED..... ID 488.223-592.328
                       X.11Y{515bb27 G.E...... .....ID 0.0-1080.1794 #7f09162f app:id/(name removed)}
                         android.widget.ProgressBar{70c1d4 G.ED..... 513,870-566,923}
                         X.1Et{9094f7d V.ED..... ID 0.0-1080.1794 #7f09190d app:id/(name removed)}
                   X.4ZD{6dd1e72 V.E..... 0,191-1080,328 #7f090db5 app:id/(name removed)}
                     X.1SZ{998e2c3 V.ED..... 31,26-396,111}
                     android.view.View{1022740 V.ED..... 396,0-944,0}
                     X.1Hi{1606679 G.ED..... I. 0.0-0.0}
                     X.1Hj{fdaafbe VFED..C.. ..... 944,5-1070,131}
                     X.1Hj{c9ce81f G.ED..... .....I. 0,0-0,0}
                   android.widget.FrameLayout{4d76fb2 V.E..... 5400,0-6480,1794 #1020002 android:id/content}
                   android.widget.FrameLayout{96efb03 V.E..... 0,0-1080,1794 #7f090f25 app:id/(name removed)}
                   android.view.ViewStub{577f135 G.E...... 0,0-0,0 #7f092747 app:id/(name removed)}
                   android.view.ViewStub{38e09ca G.E...... I. 0.0-0.0 #7f092980 app:id/(name removed)}
                android.view.ViewStub{7994c37 G.E..... 1. 0,0-0,0 #7f09009d app:id/(name removed)}
              android.view.View{5294cbf V.ED..... 0,1794-1080,1794 #7f091a7d app:id/(name removed)}
              X.1Di{73d42de V.E..... 0.0-1080.328 #7f09116b app:id/(name removed)}
                X.1Db{2b20f8c V.E..... 0.0-1080,328 #7f09116a app:id/(name removed)}
                 X.1qn{f369878 V.E..... 0,63-1080,328 #7f091167 app:id/(name removed)}
                   X.1Di{183ab51 V.E..... 0.0-1080.137 #7f092921 app:id/(name removed)}
                     X.2HG{178c424 VFE...C.. ...... 0,0-1080,137 #7f092920 app:id/(name removed)}
                       X.2HH{b2a3142 V.ED..... 32.0-347.137}
                       android.view.View{406ab8d V.ED..... 347,0-817,0}
                       X.2HH{7054553 VFED..C.. 817,0-943,126 #7f092347 app:id/(name removed)}
                       X.1Hj{98ffe90 VFED..C.. ...... 943,0-1069,126 #7f09023a app:id/(name removed)}
                     android.view.ViewStub{b0865a4 G.E...... .....I. 0,0-0,0 #7f092746 app:id/(name removed)}
                   X.1Di{4e8cfb6 V.E..... 0,137-1080,263 #7f0927fd app:id/(name removed)}
                     X.1BD{62e1f8e V.E..... 0,0-1080,126 #7f0927fb app:id/(name removed)}
                       X.1Hi{514e3af VFED..CL. ..S..... 0,0-180,126 #7f0918f4 app:id/(name removed)}
                       X.1Hi{f9e73bc VFED..CL. ....... 180,0-360,126 #7f090f68 app:id/(name removed)}
                       X.1Hi{d22bf45 VFED..CL. ....... 360,0-540,126 #7f092abe app:id/(name removed)}
                       X.1Hi{270a69a VFED..CL. ...... 540,0-720,126 #7f0928fc app:id/(name removed)}
                       X.1Hi{1d60bcb VFED..CL. ...... 720,0-900,126 #7f091937 app:id/(name removed)}
                       X.1Hi{9bd0fa8 VFED..CL. ...... 900,0-1080,126 #7f0903f3 app:id/(name removed)}
                     X.1Dh{53f7389 V.E..... 0,0-1080,126 #7f0927fe app:id/(name removed)}
                   android.view.View{32e14b7 V.ED..... 0.263-1080.265 #7f0927fc app:id/(name removed)}
                X.1B4{8d576d5 V.E..... 0,283-1080,326 #7f0927f9 app:id/(name removed)}
                                             T 0 42 4000 42 #76002760 200.14//0200 commend)
                  V ADAFORFEELL W.F.
```

### III. Hide view IDs: Implementation

Method 1: View wrapper

```
public class MyTextView extends TextView {
   public MyTextView(Context context) {
        super(context);
   // works on uiautomatorviewer
   @Override
   public void onInitializeAccessibilityNodeInfo(AccessibilityNodeInfo info) {
        super.onInitializeAccessibilityNodeInfo(info);
        if (Build. VERSION. SDK INT >= Build. VERSION CODES. JELLY BEAN MR2) {
            info.setViewIdResourceName("(name removed)");
```

### III. Hide view IDs: Implementation

Method 2: Resources wrapper

```
public class CustomResources extends Resources {
    public CustomResources(Resources res) {
        super(res.getAssets(), res.getDisplayMetrics(), res.getConfiguration());
    // works on uiautomatorviewer
   @Override
    public String getResourceName(int resid) throws NotFoundException {
        return "(name removed)";
    // works on "adb shell dumpsys activity top"
   @Override
    public String getResourceEntryName(int resid) throws NotFoundException {
        return "(name removed)";
```

## IV. Extra tips

- Dynamic code
- Detect rooted device
- Detect rom debug
- Encrypt resources
- Store important resources on server

### References

https://developer.android.com/studio/build/shrink-code

https://android-developers.googleblog.com/2018/11/r8-new-code-shrinker-from-google-is.html

https://www.guardsguare.com/en/products

https://www.guardsquare.com/en/products/proguard/manual/usage

https://www.guardsguare.com/en/blog/proguard-and-r8

https://source.android.com/setup/build/building

# Thank you for listening!

