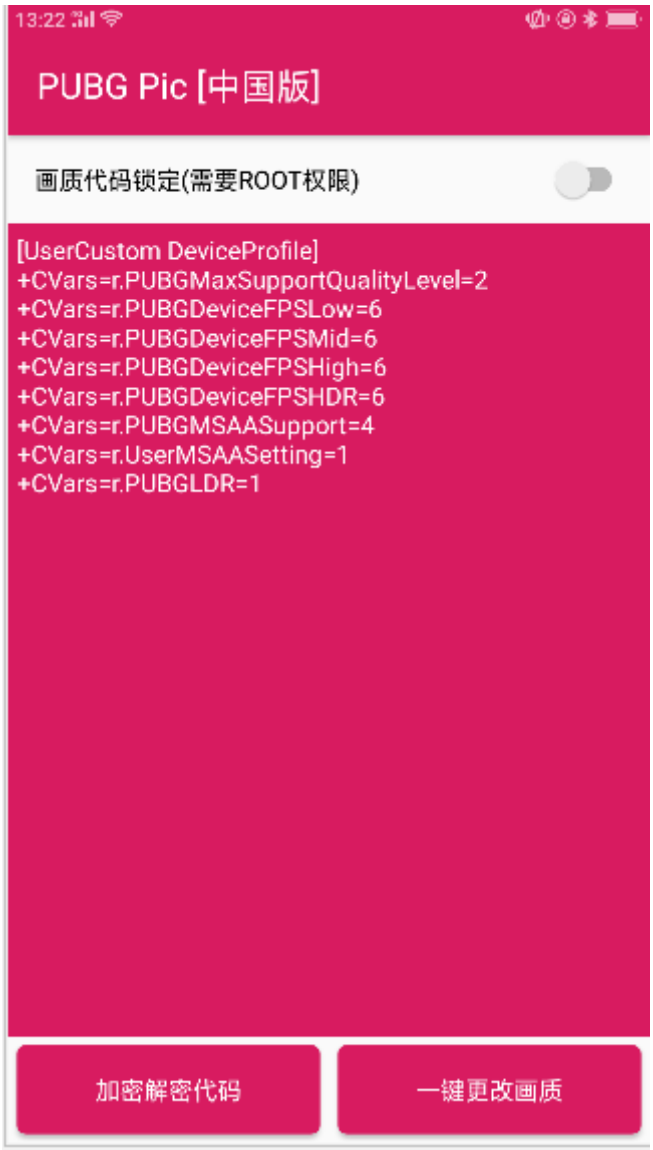
逆向gfx tool 第三天

笔记本:	gfx逆向		
创建时间:	2019/11/9 13:17	**更新时间:**	2019/11/13 21:52
作者:	381643188@qq.com		
URL:	https://www.jianshu.com/p/138c9de2c987		

背景

这次我们先实现一个完整功能的gfx工具，来修改吃鸡参数。之前的方法有点不够高效和明了。我们发现有款工具也可以修改参数，并且可以把加密过的参数进行解密和重新加密。这点是我们需要的。
所以就需要对这个功能进行反编译。


13:22
PUBG Pic [中国版]
画质代码锁定(需要ROOT权限)
[UserCustom DeviceProfile]
+CVars=r.PUBGMaxSupportQualityLevel=2
+CVars=r.PUBGDeviceFPSLow=6
+CVars=r.PUBGDeviceFPSMid=6
+CVars=r.PUBGDeviceFPSHigh=6
+CVars=r.PUBGDeviceFPSHDR=6
+CVars=r.PUBGMSAASupport=4
+CVars=r.UserMSAASetting=1
+CVars=r.PUBGLDR=1
加密解密代码
一键更改画质


13:22
PUBG Pic [中国版]
画质代码锁定(需要ROOT权限)
[UserCustom DeviceProfile]
+CVars=0B57292C3B3E3418012A0C0909160B0D280C1
+CVars=0B57292C3B3E3D1C0F101A1C3F292A35160E4
+CVars=0B57292C3B3E3D1C0F101A1C3F292A34101D4
+CVars=0B57292C3B3E3D1C0F101A1C3F292A31101E1
+CVars=0B57292C3B3E3D1C0F101A1C3F292A313D2B4
+CVars=0B57292C3B3E342A38382A0C0909160B0D444
+CVars=0B572C0A1C0B342A38382A1C0D0D10171E444
+CVars=0B57292C3B3E353D2B4448

先用APKTool

解开后搜索字符串“加密解密代码”。结果为:

```
<string name="button1">加密解密代码</string>
<string name="button2">一键更改画质</string>
```

再使用Jadx

这个apk使用了奇虎360的安全加固，一部分信息直接丢失了，所以无法反编译java文件。

再回到apk_tool

所以这里直接使用apk的的结果先进行查看。使用button1字符串的按钮为

```
<Button android:textColor="#ffffffff"
android:android:background="@drawable/button_edge"
android:layout_width="fill_parent" android:layout_height="50.0dip"
android:layout_margin="5.0dip" android:foreground="?
android:selectableItemBackground" android:text="@string/button1"
android:layout_weight="1.0" />
```

他的id为

```
 <public type="id" name="button3" />
```

转换为十进制为2131230762。
搜索不到，发现apktool也也不能正确解压出smali文件。这块有点牛逼呀。需要仔细研究一下，怎么破解呢。

大概看了一下，奇虎应该是对dex动了手脚，dex总共大小为1M，但是破解出来就只有8个类。

还是不行，笨办法

那就只能先用加密后的字符串直接写了。

每一串命令前边都是固定的，后边是可变的参数，表示不同的选项。所以我们通过对比可以获得前半段的数据，再通过破解获取后半段可变参数的数据。可以省去很多重复工作量。

想了想，我还是先分析一下上次破解的加密函数，看能不能发现什么。

额。。。貌似没发现什么。

算了，还是硬来吧，先确定后边，再确定前边，这样更快一些。

最后发现还是不行。

破解360

这里使用VirtualXposed + FDex2进行脱壳，得到com.pic.pubg里边的两个dex，反编译后发现了AddCode，可以将UserCustom.ini的内容翻译成明文。这里重大突破。