Android应用反编译

反编译 apktool dex2jar

Android应用程序APK文件其实就是一个MIME为ZIP的压缩包，我们修改ZIP后缀名方式可以看到内部的文件结构，类似Sun JavaMe的Jar压缩格式一样，不过比较去别的是Android上的二进制代码被编译成为Dex的字节码，所有的Java文件最终会编译进该文件中去，作为托管代码既然虚拟机可以识别，那么我们就可以很轻松的反编译。所有的类调用、涉及到的方法都在里面体现到，至于逻辑的执行可以通过实时调试的方法来查看，当然这需要借助一些我们自己编写的跟踪程序。

我们将apk文件解压后有两部分文件需要处理，一种是xml文件，另一种一个dex文件（.dex），我们可以从.dex文件中得到.class，利用后者再得到大家垂涎已久的java文件。

- **xml反编译apktool**

```
*setp1*
cd 进入到存放aapt.exe、apktool.bat、apktool.jar的文件夹
*step2*
apktool d [-s] -f <apkPath> -o <folderPath>,参数具体的意思可以直接打
apktool回车(windows)查看帮助
*step3*
此时在输出的文件folderPath中就可查看所有资源文件（xml和图片）
```

> 中途遇到的问题
> 1. `Exception in thread "main" brut.androlib.AndrolibException: Could not decode arsc file;Caused by: java.io.IOException: Expected: 0x001c0001, got: 0x00000000`
> 解决方案：可能由于工具版本太旧，登陆http://code.google.com/p/android-apktool/wiki/DownloadInstructions?tm=2下载最新版本的apktool.jar，目前最新版本为2.0.0 RC4
> 2.反编译 `Input file was not found or was not readable`
> 解决方案：命令格式 apktool d [-s] -f < apkPath > -o < folderPath>

此时就可以看xml文件了

- **dex反编译dex2jar**
  java文件编译过程java->class->dex;反编译过程dex->jar->class->java;dex编译成jar需要根据dex2jar,而jar到java的 编译时基于JDcore引擎衍生的一些工具
  1.下载一步到位反编译apk工具(onekey decompile

apk)：https://github.com/ufologist/onekey-decompile-apk
2.将下载的onekey-decompile-apk.zip, 解压缩到类似 D:\downloads\onekey-decompile-apk
3.将apk文件放到onekey-decompile-apk目录下
4.将apk文件拖拽到_onekey-decompile-apk.bat上
执行完成后（ `注意:批处理文件打不开，只需将apk拖到批处理文件上运行即可` ）
5.会在onekey-decompile-apk目录下生成和apk同名的目录(放置了apktools反编译出来的东西)
6.会在onekey-decompile-apk目录下生成和apk同名的jar文件(dex2jar反编译出来的class)

如果不想用这个一键生成工具，也可以一步一步来操作

- **dex2jar:将classes.dex转变成jar**
  1.首先找到APP软件安装包中的classes.dex（解压得到）;它就是java文件编译再通过dex工具打包成的,所以现在我们就用上述提到的2个工具来逆方向导出java源文件
  2.把classes.dex拷贝到dex2jar.bat所在目录;在命令行模式下定位到dex2jar.bat所在目录，运行

```
dex2jar.bat classes.dex
```

此时就生成了classes.dex.dex2jar.jar，成功了一半！

- **JD-GUI：将jar转化为java文件**
  1.下载JD-GUI,解压得到JD-GUI，用它打开上面的jar文件，File–>Save JAR Source，即可看到梦寐以求的java源代码.
  2.此时看到的源代码有可能是混淆过的，如出现A类、B类（人家也是为了保护自生权益嘛）。

> 执行完上述操作后就可以得到相应的java文件了