**免ROOT框架TweakMe介绍(二)**

TweakMe是一个轻量级的逆向开发框架，它与传统的xposed、frida、magisk等框架相比的最大优势是无需root环境，对手机系统的要求很低，只需要一个正常手机即可对app进行逆向分析。简单的几步操作就可以完成对指定app的进程注入，可以绕过大多数加固(360、梆梆、爱加密等)的签名证书校验。完成注入后通过Java编写hook代码，一键脚本编译为dex插件。目前TweakMe框架在5.0到11.0的android手机上测试通过。

本文档主要介绍TweakMe 2.0的新特性，如果你已经对TweakMe有所了解，请继续往下看，如果你是首次接触它，请先看《免ROOT框架TweakMe介绍》

TweakMe地址：**<https://git.17usoft.com/TweakMe/TweakMe>**

**<https://github.com/liaoguobao/TweakMe>**

强烈建议在非ROOT的正常手机上使用本框架

一、反签名校验能力增强

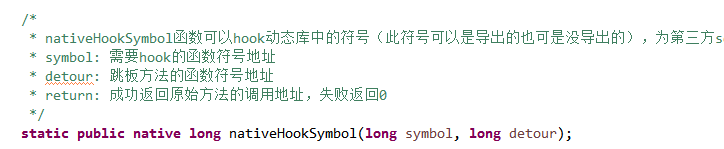
由于框架对原始apk做过调整，反签名校验是本框架的核心功能，2.0版本大大增强了这方面的能力。如果在点击app图标后直接闪退（前提是没有流程操作上的错误），那大概率就是反签名校验失败，被加固厂商的so直接kill掉了。如果在1.0版本上出现过这个问题，不妨在2.0上再试一次，可能会有惊喜哦！

二、增加了一个sodemo目录

目录中包含了一个so开发的小demo。考虑到许多朋友不仅要开发java插件，还可能需要开发so插件，所以做了一个小例子供大家参考。主要是展示如何hook动态库中的函数。此demo需要自行用NDK编译，由于NDK版本太多（本人用的比较旧的ndk-r13b版本），所以在编译过程中出现的版本错误请大家自行修正。

1. 支持native层符号hook

为了支持native层符号hook，在JavaTweakBridge类中新增如下方法：



需要注意的是，此方法并不是用来拦截java层的native方法的，而是用来拦截native层的各种符号函数或者过程的（IDA中以sub\_xxxx这种形式显示）。具体使用请看函数说明，以及sodemo中的使用例子。

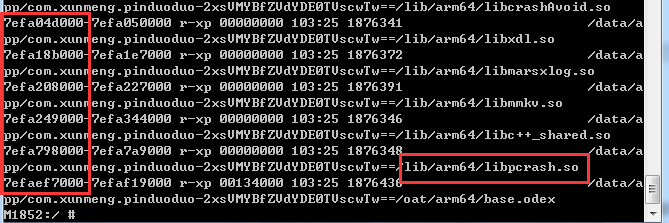
1. 使用问题总结
2. 编译环境需要准备哪些

如果想编译java插件，必须要安装java环境，建议安装java1.8。如果想编译sodemo，必须要安装NDK。如果想查看运行日志，必须要安装ddms，这个工具在安装了AndroidStudio或EclipseForAndroid之后会自动安装。

1. 如何确定需要注入的目标so

对于加固的APP，目标so就是加固so本身，每个第三方加固商都有对应的固定so名称，直接百度搜集即可。对于没有加固的app，大家可以查看/proc/$PID/maps文件，基地址最大的so即是第一个被加载的so。

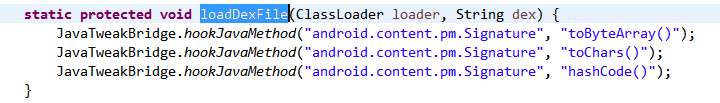
如下图所示（必须要在root过的手机上才可以看maps文件）



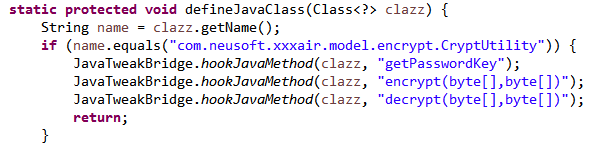
libpcrash.so的基地址被映射的最大，可以尝试做为目标so

1. 应用层java方法如何hook，在哪里写hook代码

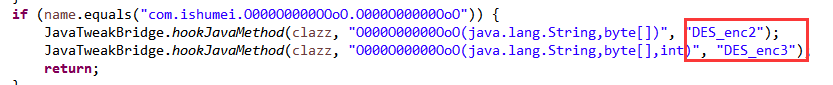
对于android.jar中实现的系统方法，建议在loadDexFile函数中hook



对于具体应用层的java方法，比如数据加解密相关的、请求包相关的方法，应该在defineJavaClass回调中hook，采用如下形式



如果需要hook类中的重载方法，一定要写明参数列表，对于混淆的方法，可以指定一个友好的方法名称。如下图



1. 有没有所有文件（so\dex）全内嵌apk的版本

目前没有，放置在apk外面，是方便修改，内嵌在apk里面每次修改都要重新打包，重新安装，很不方便。

1. 重打包完成后是否还可以调整包内容

可以，比如可以把libsodemo.so这个动态库放入lib/$ABI目录中，再--sign命令重新签名一次。

1. 签名数据设置是否只能调用setAppCert函数，有其它简单方法吗

setAppCert每次都需要调用，这样可以不必修改JavaTweak\_sign.java的代码。另外如果直接将签名数据放置到JavaTweak\_sign.java的***SIGN\_BASE64***变量中，则可以不必调用此函数了，格式如下图所示



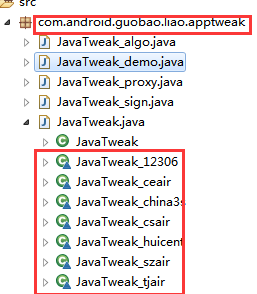
1. 自己想要hook的类没有在defineJavaClass中回调如何hook方法

首先如果是android.jar中的系统类的话，是不会回调的，可以直接hook的到。

如果是应用层的类出现不回调的话，可以在同一个包中兄弟类加载的时候hook目标类。写法如下



1. 自己新建一个java插件类需要注意什么？
2. 必须要放在com.android.guobao.liao.apptweak包中
3. 类名必须要以JavaTweak\_开头



C、loadDexFile、defineJavaClass必须要至少实现其中一个，如下图的demo插件

