**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>**

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

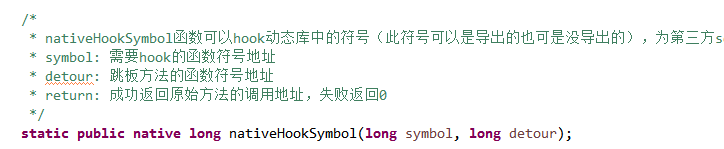
由于框架对原始apk做过调整，反签名校验是本框架的核心功能，2.0版本大大增强了这方面的能力。如果在点击app图标后直接闪退（前提是没有流程操作上的错误），那大概率就是反签名校验失败，被加固厂商的so直接kill掉了。如果在1.0版本上出现过这个问题，不妨在2.0上再试一次，可能会有惊喜哦！

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。