安卓证书锁定解除的工具

瘦蛟舞 (/u/7137) / 2018-03-05 11:39:49 / 浏览数 14046

地址：https://github.com/WooyunDota/DroidSSLUnpinning (https://github.com/WooyunDota/DroidSSLUnpinning)

经常有朋友问我,手机安装代理证书后这个app的https流量依然抓不到包该如何操作,这样情况基本是遇到证书锁定了,分享下我的操作.

- [x] 目录JustTrustMePlus加了些JusTrustMe没覆盖到的锁定场景.(基于xposed模块justTrustMe (https://github.com/Fuzion24/JustTrustMe)稍作修改)
  - 使用方法1：安装激活xposed后,安装目录下提供的apk,勾选jusTrustMe模块激活重启即可.

- [ ] 目录ObjectionUnpinningPlus加了些ObjectionUnpinning没覆盖到的锁定场景.(基于Frida模块objection hook pinning (https://github.com/sensepost/objection)稍作修改)
  - 使用方法1 attach : frida -U com.example.mennomorsink.webviewtest2 --no-pause -l hooks.js
  - 使用方法2 spawn : python application.py com.example.mennomorsink.webviewtest2
  - 更为详细使用方法:ToBeDone参考我的文章 Frida.Android.Practice (https://github.com/WooyunDota/DroidDrops/2018/) 实战ssl pinning bypass 章节 .

- [ ] 如遇双向锁定即客户端锁定后服务端也对客户端证书验证checkClientTrusted,还需将证书文件导入代理软件,可能会有密码但必然会存在客户端中.
- [x] 若有没有覆盖到的场景可以联系我微博https://weibo.com/luoding1991 (https://weibo.com/luoding1991).

上一篇： 某CMS 5.X版本 管理员密码重置漏洞 (/t/2097)　　下一篇： 内核驱动mmap处理程序利用（翻译） (/t/2099)

8 条回复

bma (/u/4104) **2018-03-05 14:37:02**

@瘦蛟舞 (/forum/user/7137)
表哥，用frida hook Android so中的native方法，怎么样获取、修改传入的参数值？目前可以直接调用该native方法。另外在hook时，某些apk存在反调试措施，存在两个或多个进程，导致frida无法hook，使用-f --no-pause spawn新进程时手机死机，咋办？

0　回复Ta

hades (/u/1037) **2018-03-05 14:46:42**

@bma (/forum/user/4104) 可以先楼一眼下面的文章，作者正在来的路上
https://xianzhi.aliyun.com/forum/topic/289 (https://xianzhi.aliyun.com/forum/topic/289)
https://xianzhi.aliyun.com/forum/topic/230 (https://xianzhi.aliyun.com/forum/topic/230)

0　回复Ta