看雪『Android安全』板块 2018 年优秀和精华帖分类索引

转载

擒贼先擒王 于 2020-07-31 11:59:09 发布 424 收藏 1
分类专栏： Android 逆向
原文链接：https://bbs.pediy.com/thread-249602.htm

Android 逆向 专栏收录该内容
30 篇文章 23 订阅
订阅专栏

转载：https://bbs.pediy.com/thread-249602.htm

[推荐]『Android安全』版2018年优秀和精华帖分类索引

文章筛选和评价仅代表个人观点，欢迎指正。

列表不定期更新，欢迎自荐~ 2018年

1.逆向技术基础

Frida操作手册-Android环境准备
Frida hook方便快捷，并且跨平台，可以学习一下

Brida操作指南
葫芦娃的又一篇神作，抓包，加密，解密一条龙。

介召几个frida在安卓逆向中使用的脚本以及延时Hook手法
延时hook，so，java层堆栈回溯的好文章！

学习Androidx86模拟器root安装xposed
lamHuskar告诉我们学习xposed hook不用去买一部android手机。

答"遇到接口时通过静态分析找不到实现类的时候该如何用 xposed 来定位"
来回答这篇帖子的问题遇到接口时通过静态分析找不到实现类的时候该如何用 xposed 来定位
作者讲了三种方法，来找到具体实现的java类，点此一看吧！

1.1 反调试，虚拟机检测和一些技巧

Nexus6P 7.1.2 内核编译修改 TracerPid
不多说，很实用！

[记笔记]DroidSSLUnpinning
安卓证书锁定解除的工具

检测Android虚拟机的方法和代码实现
Vancir整理的很详细，很不错的分享

2.软件破解&逆向分析

编译libc.so过time函数反调试
修改libc.so源码，实现检测time()反调试的绕过。

android ro.debuggable属性调试修改(mprop逆向)
ptrace 1号init进程进行改值。

分享一下我【解决问题】的思路和流程
junkboy的分析很有经验！

小密盾简单逆向分析

某电话轰炸机APP破解授权全过程
落魄的后生哥的这篇文章很适合入门，破解，重打包，签名，引用评论的言论：“文章感情线明暗两条，一明一暗，作者妙笔生花，均呈现出不一样的光彩，令人眼前一亮”。

记某app内购破解 – 安卓逆向菜鸟的初体验
qiantang写的非常详细，思路也较多，适合新手学习和入门。

2.1 游戏破解

cocos2d游戏里面的图片资源全都加密
图片资源如何通过ida直接挂接解密可以参考此篇。

一个 Cocos for Lua 伪网游的破解实战
很详细，领教了。

老skr江的两篇帖子可以学习unity手游的分析破解，值得推荐。
某大厂unity手游，和另一篇某易手游的对比
某厂某手游保护绕过
hook非导出函数（基址+偏移），拿到解密的dll
某易Unity客户端保护浅析与绕过
dump,寻找hook的时机

关于手游王朝崛起调试破解心得分享
u3d游戏的dll的解密修改打包。

同样nesc贡献了三篇好文！
Unity3D手游破盾之旅
got表hook+修复

再战某易的Unity3D mono保护
可以参考里面相关的思路和技术点也是不错

某Unity3D游戏加固产品分析
又一篇暴力修复dll的好文！

Unity3D mono模式游戏保护之浅谈
通过自定义PE头文件格式的加载方式进行保护，就可以防止轻易被破解了。

unity3d手游破解（一）
unity3d手游破解（二）
unity3d手游破解（三）--基于inline hook
王正飞对unity3d手游的一些分析。

2.2 脱壳技术

利用**加固逻辑漏洞取巧脱壳
字节码只要还原的壳，应用进程内读取再写入dex文件即可脱壳(hook相关io函数实现重定向)？？？！

简单apk脱壳工具源码
通过hook attachBaseContext得到壳的classloder,classloder继续hook真正类的oncreate,classloader获取内存中的所有cookie，得到dexFile，组合dex。

Android通用脱壳机FUPK3
currwin脱壳思路清晰而且有深度，经典文章，必读！

移动样本之初学脱壳
xiongcc带你手把手脱简单的壳。

---------手脱定制版的android SO UPX壳
没有太多要说的，oooAooo这篇文章极其牛叉和清晰。读者需要在了解Android linker加载机制和elf文件格式的基础上学习比较好懂。

一张表格看懂：市面上最为常见的 Android 安装包（APK）五代加固技术发展历程及优缺点比较！
五代加固技术的对比图，很全！

【脱壳一】某壳分析+修复
Roselia对dex抽取加固方案的一些分析。

【脱壳二】某最新免费壳分析+脱壳
Roselia的这篇文章介绍了早期的脱壳，或许现在有很多思路来dump原始dex，或者这个方法对目前版本也许无效了，但分析的思路和一些知识非常值得学习。

Dalvik解释器源码到VMP分析
某vmp壳原理分析笔记
glider菜鸟的这两篇文章对vmp壳的分析，思路和处理方法有学习的意义。
某壳分析学习过程-修复
360加固之onCreate函数还原并重打包
这四篇文章针对native的onCreate修复过程，值得学习。

2.3 协议分析

浅析Seafile网盘apk的端对端加密方式
了解协议分析和算法的好文！

MG初步协议分析
sqdebug的协议分析可谓精彩，从手托upx定制壳到修复，然后直接脱类抽取的壳，定位关键native函数，过反调试都很有经验！

某短视屏逆向分析

wss协议分析(SSL加密的WebSocket)
skyun带我们认识分析wss，思路严谨，逻辑清楚。

3.软件保护

upx原理分析
一个Android壳简单实现
对于了解dex初级加固，so加密指定节和指定函数有了很好的介绍。
dex vmp虚拟化
分析一个有趣的so双重壳

android so加固
liumengde简要指出了so加固的难点分析。

ollvm快速学习
七少月写此文章目地是为了从另一个从未出现的角度来让一个完全不懂llvm的新手快速上手ollvm。

4.系统漏洞分析和攻击利用

安卓内核驱动编译方法

(Android Root)CVE-2017-7533 漏洞分析和复现

2017-8890堆喷的一些思考
如题，wule思考堆喷时提高命中率，值得一看。

CVE-2015-1805 iovyroot 查找内核地址
详细讲述了提取zImage到ida查找符号的过程。

CVE-2015-3636(pingpong root) android内核 UAF漏洞分析
虽然是老的漏洞，但依然经典，houjingyi从环境搭建到最后提权，见招拆招，编译gdb....很详细！

阿里90后工程师利用ARM MMU硬件特性开启安卓8终端的上帝模式
后续的补充知识资料：KSMA -- Android 通用 Root 技术,文字如果看不懂，可对照代码看更加清晰明白，讲的获取root后，通用的适配方式。

一个内核驱动的数组越界访问漏洞

ZipperDown漏洞，炒作还是一触即发?
cve-2015-6620学习总结
glider菜鸟介绍binder的漏洞，越界实现任意地址读取和pc寄存器的控制。

CVE-2017-13258 Android 蓝牙BNEP漏洞分析
这是ID蝴蝶关于蓝牙的内存信息泄漏的分析。

QQFuzzy可能性乱扯
QQFuzzy可行性尝试二--被忽略的漏洞总结
eightmg对qq做了更详细的探索。

CVE-2017-13253 Android Drm服务 堆溢出漏洞调试分析
CVE-2015-3864漏洞利用分析(exploit_from_google)
WiFi网络WPA2 KRACK漏洞分析报告

5.系统安全与原理

一种绕过Android P上非SDK接口限制的简单方法
通过获取对象偏移修改内存或者签名，绕过调用隐藏api的限制。

简单暴力非provide式突破Android P对调用隐藏API限制的方法
七少月从正向和逆向的思路来突破和绕过。

xposed实现插件代码更新同时避免重启系统方案
virjar使用一个永远不变的class，作为加载器。这个Class的功能就是寻找最新的apk安装路径，然后构造新的classLoader，然后调用hook入口。

6.刷机技术与维护

关于手机救软砖(soft brick)的一点总结
安卓内核驱动编译方法
已经很详细了！

关于LineageOS 15.1前置摄像头无法正常使用的临时解决方案
用14.1版本的相机应用替换掉15.1版本的应用即可。

修改LineageOS 15.1源码，实现内录(已测试)

7.恶意代码分析

记一次Android后门分析实战

一个section加密的apk的分析
houjingyi对分析和调试apk的经验分享。

8.原创工具和代码

适配古河大佬的注入工具到 AndroidN+
androidN以上设备对dlopen的使用有权限检查，可以使用另外一个函数加载so,看作者longpoxin如何操作。

如何优雅的延长JEB demo的有效期
解决旧版本JEB在最新版的JDK下闪退

Null混淆
修改混淆proguard jar包，增加dex反编译工具，xpose hook难度。

MIUI稳定版刷机+部分root获取+xp安装记录

ApkAssist(Apk一键捆绑工具)
AndroidManifest.xml反编译、编译、合并，指定so DT_NEEDED注入我们的so
还有dex smali注入。

JEB2反混淆神器

微信6.6.1 Xposed模块 包含 主动发消息 防撤回 抢红包 骰子作弊 模拟位置 步数最高
skyun通过xposed实现了以上功能，源码非常全，非常赞！

9.其他安全产品分析

攻破国内某大型app抓包hook签名检测，居然只是想替它实现懒人自动下一条视频播放？
通过对话框，资源，ddms定位和页面布局进行破解入手的好文。

快过年了，最暴力的微信骰子作弊方法（附分析过程），不是hook~~~
经验代表一切，直接搜索关键词AssertTrue定位，然后smali注入，完成任务，Good good study大神带你领略美妙的操作。
修改微信余额显示
从界面字符串入手进行分析，直到smali代码，然后进行重打包，写的详尽，思路清晰，学习的好文！

修改微信实现防撤回、自动抢红包功能
iweizime通过过掉校验和资源混淆，复用微信组件和界面，调试，修改apk代码实现了以上功能，功力深厚。

10.Hook和注入

Android Hook 系列教程(二) 自己写APK实现Hook Java层函数
Android Hook 系列教程(一) Xposed Hook 原理分析
chpeagle写的很详细。

inlineHook学习分析
LOphTg对f8left和ele7enxxh写的hook项目的分析。

源码简析之ArtMethod结构与涉及技术介绍
android高版本的ArtMethod改动处，原因，以及适配点，写的很有深度。

使用frida来hook加固的Android应用的java层
从源码分析的过程很赞!

初识Frida--Android逆向之Java层hook (一)
初识Frida--Android逆向之Java层hook (二)
进阶Frida--Android逆向之动态加载dex Hook（三）（上篇)
进阶Frida--Android逆向之动态加载dex Hook（三）（下篇)
关于Frida的介绍和实战系列，ghostmazeW太棒了。

frida源码阅读之frida-java
又一篇frida之作！
Frida从入门到入门—安卓逆向菜鸟的frida食用说明
新手入门Frida的好文！

Xposed第一课(微信篇) hook含有多个参数的方法
Xposed第二课(微信篇) 聊天界面修改文字
Xposed第三课(微信篇) 防止好友消息撤回
Xposed第四课(微信篇) 朋友圈点赞 (1)
Xposed第四课(微信篇) 朋友圈点赞(2)之好友列表
Xposed第五课(微信篇) 聊天机器人__群聊小助手n(≧▽≦)n
KingZd用xposed对微信进行了分析。

Xposed__监听微信登录帐号和密码
Xposed__监听微信文本消息并关键字拦截

xposed art-runtime移植细节
可直接下载文章下的pdf阅读，文章图片不能正常显示了。

爱奇艺APP使用的 native PLT hook 库开源了，经过了“亿级”线上设备的稳定性兼容性考验
plt hook非常完善了！