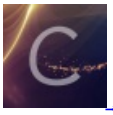
看雪论坛 『Android安全』版优秀和精华帖分类索引

转载

Omni-Space 于 2016-03-22 07:10:20 发布 1822 收藏
分类专栏： Android Security 文章标签： 看雪 Android Security


Android Security 专栏收录该内容
209 篇文章 9 订阅
订阅专栏

逆向技术基础

《 对某APK的一次分析 》
JayL的这篇分析中介绍的工具对初学者依然值得参考。

《 android一个crackme分析和破解 》
zhaokang的CrackMe 101。

《 呼叫非虫，关于Dalvik 指令格式问题 》
非虫详细解答了bdw关于Dalvik bytecode编码的问题

《 Android安全之 – Dex文件解析 》
不歪对DEX格式的详细介绍，视频！

《 Dalvik寄存器&反汇编格式视频讲解 》
还是不歪的视频教程。

《 android程序破解练习初级 》
pc小波对Android上练习用的一个KeygenMe的两种破解方法。

《 (arm入门)反汇编分析一个arm函数调用的生死因果 》

《 apk反汇编之smali语法 》
羽风的星的翻译

《 IDA Android Remote Debug 》

《 使用AndBug调试Android Java Bytecode 》
古河介绍了Dalvik无源码调试工具。

《 原生程序初次逆向之ARM与X86相关知识对比 》

《 修改Android模拟器的system分区，以及加入SuperSU 》

软件破解

《 APK Crack 》
ZhWeir早期的一些思路。

《 AD Blocker Trial 注册算法 》
iltgcl这篇文章思路自然清晰。

《 AD Blocker Trial 破解小记 》
我是土匪的一篇软件破解文章。

《 DIY新浪微博Android手机客户端（一）（二）（三）完 》
aqtata的这篇文章介绍了如何把早期新浪微博客户端通过重打包的方法来欺骗服务器，使之认为是iPhone客户端等。这个方法对目前版本的微博也许无效了，但重打包和数据分析的思路非常值得学习。

《 [有新手指引]陌陌跳过apksign验证方法 》
alice对陌陌的客户端签名信息验证，用伪造的方法进行了绕过

《 逆向iReader解读ebk2电子书格式 》
荒野无灯这篇文章应该是本版第一篇对私有格式的逆向。

《 Android下ARM静态反编译逆向.(小试多玩YY协议) 》
alice的这篇文章则是第一篇关于私有协议逆向的。

《 微曝光两个安卓腾讯应用的细节 》
bakurise对私有加密方法的逆向。

《 apk破解之“异常”破解 》
zpsemo对利用异常实现验证的一个软件做了破解。

《 Android程序开机启动杀手Autorun Manager破解 》
《 海卓apn去广告破vip 》
荒野无灯降解得非常详细。

《 第一枚ARM汇编版CrackMe分析 》
《 第二枚ARM汇编程序分析 》
Speeday干得好！

《 发几篇Android方面的文章 》
《 发几篇Android方面的文章(第二弹) 》
非虫的经典文章系列，必读。

《 微信5.0 Android版飞机大战破解无敌模式手记 》
ZhWeir作品之一。可惜还是重打包。

《 MIUI收费主题破解交流 》

《 Android软件去广告方法总结[2012.3.6更新工具] 》
我是土匪带来的经验总结和ApkTool_GUI工具分享。

《 逆向过程中分析的Android APK 自校验和APK 扩张文件下载流程(visio格式图) 》

《 《我叫mt》数据包解包记录 》
风の忆带来精彩的动态分析实例。

软件保护
《 APK反破解之一：Android Java混淆(ProGuard) 》
《 APK反破解之二：Android APK 签名比对 》
《 APK反破解之三：NDK编译.so动态库 》
《 APK反破解之四：Android代码动态加载技术 》
ZhWeir对四种软件反破解技术的介绍。虽然是早期内容，目前看起来显得过于简单，但对普通软件来说，依然有值得采纳之处。

《 Android APK加壳技术方案【1】 》
《 Android APK加壳技术方案【2】 》
jiazhijun的两篇文章，由于一些原因原帖已经被作者本人删除，这里是转载。

《 梆梆加固apk的一点思考 》
羽风的星对梆梆加固方案的一些分析。

《 Andorid APK反逆向解决方案---梆梆加固原理探寻 》
jiazhijun对梆梆做了更详细的探索。

《 Apk伪加密实现与破解JAVA源码 》
zerofile贴出了大量的代码实现APK伪加密。

《 APK伪加密制作和解密 》

《 运行时自篡改dalvik字节码delta.apk原理解析（逆向） 》
Xbalien对Dalvik运行时自修改的原理做了细致地分析。

《 利用文件系统漏洞阻止 apktool,baksmali 反汇编apk 》
baksmali（好名字！）提供的有趣思路。

《 安卓加密壳 apkprotect 分析 》

《 Android DEX安全攻防战 》
jiazhijun翻译的DEX反静态分析PPT。

系统漏洞分析和攻击利用

《 Android root源代码剖析--基于CVE - 2010 - EASY 》
《 结合init源码剖析android root提权漏洞（CVE-2010-EASY） 》
androider对CVE-2010-EASY提权漏洞的两篇分析。还有一个后续博文：
《 《android提权漏洞CVE-2010-EASY修复》 》

《 安卓下的download&exec 》
《 有关安卓shell反弹 》
pdx这两篇文章都是关于在Android 2.0/2.1下利用WebView的CVE 2010-1119 UAF漏洞一些技术细节。

《 Android系统shellcode编写 》
promsied的这篇教程精彩而详尽

《 Android adb setuid提权漏洞的分析 》
Claud基于RageAgainstTheCage源码对adb setuid提权漏洞的原理分析

《 Android提权代码zergRush分析 》
Claud结合zergRush.c源码对相关提权漏洞的原理分析。

《 Android本地生成PDU伪造任意短信代码（支持中文GSM_UCS2） 》
作者木桩对Android本地短信伪造漏洞的利用代码进行了修改，使之支持中文内容。

《 Android操作系统安全研究系列——键盘记录 》
hacknet提出的一种攻击方法，这种方法导致淘宝等客户端改变安全策略，开始在Android上使用内置虚拟键盘输入密码。

《 如何绕过Google Nexus One手机Bootloader的数字签名检测 》
没有太多要说的，xee这篇文章极其牛叉和清晰。

《 Android下通过root实现对system_server中binder的ioctl调用拦截 》
同样不用多说的好文章。

《 一些OEM的厂商的漏洞分析 》
wdynasty对一篇相关报告的翻译。

《 Android屏幕解锁图案破解 》
gamehacker介绍了锁屏穷举这个经典攻击。

《 【非原创】Android屏幕解锁图案破解 Python代码 》

《 Android屏幕解锁图案破解 C++代码 》

《 Bluebox Security最新提报Android漏洞的初步探讨 》
ZhWeir在Master Key漏洞细节公布之前的一些探索。

《 Bluebox Security提报Android 绕过应用签名认证漏洞原理 》
jiazhijun对MasterKey的分析

《 ANDROID-8219321漏洞、POC及其他相关信息汇总 》
ZhWeir补上对MasterKey的分析和资料。

《 发个Android平台上的注入代码 》
古河大作！

《 运行时自篡改dalvik字节码delta.apk原理解析（逆向） 》
Xbalien对Bluebox公布技术的逆向分析。

《 Android安全分析挑战：运行时篡改Dalvik字节码 》
jiazhijun则对原文做了翻译。

《 android webview 漏洞背后的节操 》
superhei哥的非技术文章，一个webview漏洞，暴露出国内生态体系的诸多问题。

《 CVE-2012-4220之利用 》
tewilove（我还是喜欢你中文ID）带来精彩的高通芯片漏洞利用代码。

系统安全机制

《 手机root也安全 》
《 SEAndroid之IPC 》
安卓安全小分队对SEAndroid的介绍

《 android 4.2 安全新特性 》
wdynasty对一篇官方文档的翻译。

《 ADB安全 》

软件漏洞与安全开发

《 移动即时通讯软件安全分析-米聊 》
《 手机版MSN用户帐号安全性分析及通过网络数据包还原用户密码 》
我是土匪发现和介绍了米聊客户端早期版本的客户端验证的一个安全问题，以及MSN客户端密码明文传输问题。

《 浅谈Android软件安全自动化审计 》
泉哥关于Android客户端安全审计的笔记和经验分享

《 android客户端测试checklist 》
kindsjay写的Android客户端安全checklist，既可以用来挖漏洞，也可以给开发者自检。

《 Google安全团队对Android安全的建议 》
wdynasty对Google I/O上安全开发报告的翻译。

《 新浪微博Android客户端SSO授权认证缺陷 》
从这个角度分析的人不多，ZhWeir太棒了。

恶意代码分析

《 android的一款自释放root型恶意软件分析 》
《 一款android bot分析 》
icefisher对两个Android恶意代码的分析报告，非常经典和详细。

《 Android 沙盘原理与实现 》
泉哥自己实现的一个Android Sandbox

《 Trojan-Spy.AndroidOS.Zitmo.a病毒分析 》
pc小波一篇格式清晰的分析。

《 Android下载者分析 》
思路有点乱。

《 android木马Phone_spy分析报告 》
zhaokang的分析，里面的混淆很有趣。

《 恶意代码plankton分析记录（1） 》

《 【翻译】Android Malware (SpringerBriefs in Computer Science) 第二章节 》

原创工具和代码

《 Apk修改利器：ApkToolkit v2.1 》

《 ApkTool-GUI1.3.5内测版下载 》

《 apkprotect（免费android代码混淆、加密保护工具）版本v0.3.6 2013.9.29更新 》

《 安卓加密壳（dexcrypt) , 防止apktool,dex2jar 等工具逆向你的apk，附上下载地址 》

《 APK可视化修改工具：APK改之理（APK IDE） 》

《 通过Android重打包加固APK拦截软件行为 （源码） 》
Xbalien的工作文档和源码齐全，非常赞！

其他安全产品分析

《 手机毒霸去广告功能分析一：总体分析 》

《 手机毒霸去广告功能分析二：广告View的识别 》
《 手机毒霸去广告功能分析三：java代码（dex）注入 》
《 乐安全内嵌广告屏蔽原理 》
《 Android手机安全软件之电话拦截功能浅析 》
《 Android手机安全软件之设置电话拦截返回音浅析 》
安卓安全小分队的经典系列文章。

《 android 企业级安全新思路（Ⅰ） 》
《 android 企业级安全新思路（Ⅱ） 》
wdynasty对三星Knox等BYOD产品的笔记。

《 Android Java虚拟机拦截技术分析 》
又一篇对金山毒霸的分析。

《 Android沙盒开发之TaintDroid分析(1) 》

《 洗大师的原理 》

其他

《 如何调用Android隐藏API 》

《 三行代码获取特定广播的所有接收者 》

《 发一个为android设备搭建vpn服务器的文章 》