Android APK加固技术方案调研

简 by asce1885, jianshu.com

@author ASCE1885的 Github 简书 微博 CSDN

最近项目中需要实现自己的APK加固方案，因此就有了这一篇调研报告。

软件安全领域的攻防向来是道高一尺魔高一丈，攻防双方都处于不断的演变和进化过程中，因此软件加固技术需要长期持续的研究与投入。

目前成熟的第三方解决方案

1. 娜迦

针对Android平台下的APP被逆向分析，破解，植入木马病毒后，用户敏感信息泄露或者被钓鱼网站劫持，NAGA Android保护采用防止静态分析与防止动态调试全面防护的思路，在未保护程序运行的不同周期采取不同程度的加固措施，可以针对银行、基金、券商，电商等需在线支付领域及游戏领域，提供定制型APP安全解决方案。

主要实现：

- 类抽取：保护dex文件，防止静态分析及动态破解
- 代码加解密：保护so文件，防止静态破解
- 网络访问控制：保护so文件，拦截恶意广告，阻止注入型木马
- 敏感文件检测：保护so文件，防止静态调试
- 整体包裹：保护dex文件，防止静态破解
- 利用重定位清除ELF头：保护so文件，利用系统机制ELF头已经被系统清除，不兼容X86处理器
- 字符串表加密：保护so文件，防止静态破解
- 检查核心库：保护so文件，防止功能性数据库被劫持
- 检查调试器：保护so文件，防止动态调试

- Xposed检查：保护so文件，防止so文件，防止静态调试，防dump 防xposed脱壳神器对加固apk进行一键脱壳
- 防止跟踪：保护so文件，防止动态跟踪
- 强力清除ELF头：保护so文件，防止静态分析
- 中间码乱序：保护smali文件，dex保护，防止静态分析，不兼容Android5.0 ART模式
- 重定位加密壳段：保护so文件，对抗静态分析
- 壳完整性检查：保护so文件，防止对APP程序中的壳段进行修改、调试 兼容性100%

扩展阅读：娜迦社区

2. 爱加密

爱加密主要功能：

1. 漏洞分析：

- 文件检查：检查dex、res文件是否存在源代码、资源文件被窃取、替换等安全问题
- 漏洞扫描：扫描签名、XML文件是否存在安全漏洞、存在被注入、嵌入代码等风险。
- 后门检测：检测App是否存在被二次打包，然后植入后门程序或第三方代码等风险。
- 一键生成：一键生成App关于源码、文件、权限、关键字等方面的安全风险分析报告。

2. 加密服务：

- DEX加壳保护：DEX文件加壳保护对DEX文件进行加壳防护，防止被静态反编译工具破解获取源码。
- 内存防dump保护：防止通过使用内存dump方法对应用进行非法破解
- 资源文件保护：应用的资源文件被修改后将无法正常运行
- 防二次打包保护：保护应用在被非法二次打包后不能正常运行。
- 防调试器保护：防止通过使用调试器工具(例：zjdroid)对应用进行非法破解
- 多渠道打包：上传1个APK，通过选择android:name和填写android:value来实现对每一个渠道的包的生成和加密
- 漏洞分析服务：漏洞分析采用文件检查、漏洞扫描、后门检测等技术方向对APK进行静态分析并支持一键生成分析报告
- 渠道监测服务：监控国内400多个渠道市场入口，对应用的各渠道的下载量、版本信息、正盗版进行一站监控

- 签名工具：爱加密提供纯绿色签名工具，支持Windows、Linux和MAC系统，同时支持批量签名
- DEX专业加壳保护：本服务是对安卓DEX文件进行加壳保护，有效防止所有静态调试器对APK进行破解
- DEX专业加花保护：本服务对安卓DEX文件进行加入花指令(无效字节码)保护
- 资源文件指纹签名保护：对资源文件指纹签名进行验证保护，有效防止资源文件被篡改
- 高级防二次打包保护：本服务对APK进行防止二次打包保护，防止APK被使用非法手段修改替换文件后进行二次打包
- 高级防调试器保护：防止通过使用调试器工具(如：zjdroid、APK改之理、ida等)对应用进行非法破解
- 高级内存保护：本服务是对内存数据的专业高级保护，可防止内存调试，防止通过dump获取源码，防止内存修改
- 截屏防护：防止黑客通过截屏形式获取应用账号、应用密码、支付银行卡号、支付银行卡密码,支持安卓所有机型
- 本地数据文件保护：对APK应用的网络缓存数据、本地储存数据(提供SDK)进行深度保护
- 源码优化：1) 一键清除Log（开发日志）信息；2) 一键优化减少加密后增大的源用包大小
- 防止脚本：本服务爱加密提供防止脚本SDK，用户根据开发帮助文档进行二次开发，此保护项可有效防止游戏非法使用脚本
- 防止加速器：防止游戏使用加速器，破坏游戏公平(如：防八门神器和葫芦侠中的加速器功能)
- 防止模拟器运行：防止模拟器非法运行（可以防止运行在PC上的任何类型的android模拟器）
- 防止内购破解：防止游戏被内购破解（如：游戏内部有支付项，可以防止支付项相关内容被破解）
- SO文件保护：so文件专业保护，对so文件进行优化压缩、源码加密隐藏、防止调试器逆向分析

3. 渠道监测：

- 渠道数据监控
- 精准识别渠道正盗版
- 盗版APP详情分析

扩展阅读：加密资讯

3. 梆梆加固

提供的移动应用保护服务：

- 防逆向保护：以加密代码的方式阻止反编译，从而防止被窃取代码和创意
- 防篡改保护：通过对app的完整性保护，防止app被篡改或者盗版
- 反调试保护：阻止应用运行中被动态注入，防止被外挂，木马偷窃账号密码，修改交易金额等
- 存储数据加密保护：更底层，跨文件格式的数据加密，防止应用数据被窃取
- 环境监测和保护：云监测设备环境，防止盗版应用，恶意应用的钓鱼攻击

扩展阅读：安全SDK下载

4. 360加固保

加固保为移动应用提供专业安全的保护，可防止应用被逆向分析、反编译、二次打包，防止嵌入各类病毒、广告等恶意代码，从源头保护数据安全和开发者利益，主要提供：

- 反篡改：通过签名校验保护，能有效避免应用被二次打包，杜绝盗版应用的产生
- 反窃取：对内存数据进行变换处理和动态跟踪，有效防止数据被获取和修改
- 反逆向：对代码进行加密压缩，可防止破解者还原真实代码逻辑，避免被复制
- 反调试：多重手段防止代码注入，可避免外挂、木马、窃取账号密码等行为

[总结] 常见app漏洞及风险

静态破解：

通过工具apktool、dex2jar、jd-gui、DDMS、签名工具，可以对任何一个未加密应用进行静态破解，窃取源码。

二次打包

通过静态破解获取源码，嵌入恶意病毒、广告等行为再利用工具打包、签名，形成二次打包应用。

本地储存数据窃取

通过获取root权限，对手机中应用储存的数据进行窃取、编辑、转存等恶意行为，直接威胁用户隐私。

界面截取

通过adb shell命令或第三方软件获取root权限，在手机界面截取用户填写的隐私信息，随后进行恶意行为。

输入法攻击

通过对系统输入法攻击，从而对用户填写的隐私信息进行截获、转存等恶意操作，窃取敏感信息。

协议抓取

通过设置代理或使用第三方抓包工具，对应用发送与接收的数据包进行截获、重发、编辑、转存等恶意操作。

[总结] Android app加密保护核心概念

防内存窃取

防止通过gdb、gcore，从内存中截取dex文件，获取代码片段，从而反编译还原APK进行不法操作。

防动态跟踪

防止通过ptrace调试进程，跟踪、拦截、修改正在运行的应用，进行动态注入，保护程序运行安全。

防逆向分析

防止通过APKTool、IDA Pro等反编译工具破解DEX文件，从而获取APK源代码，保护代码层安全。

防恶意篡改

校验APK完整性，自动终止运行被篡改的APK，二次打包后应用都无法使用，杜绝盗版应用的出现。

存储数据加密保护

更底层，跨文件格式的数据加密，防止应用数据被窃取。

［我们的措施］Android程序反破解技术

对抗反编译

对抗反编译是指apk文件无法通过反编译工具（例如ApkTool，BakSmali，dex2jar等）对其进行反编译，或者反编译后无法得到软件正确的反汇编代码。

基本思路是寻找反编译工具在处理apk或者dex文件时的缺陷，然后在自己的代码中加以利用，让反编译工具在处理我们apk文件的时候抛出异常或者反编译失败，有两种方法可以找到反编译工具的缺陷：

- 阅读反编译工具的源码
- 压力测试

对抗静态分析

反编译工具一直在改进，因此即使你在版本2.1发现它的缺陷并加以利用，使反编译你的apk失败，但很可能在版本2.2就把这个缺陷解决了，因此，不要指望反编译工具永远无法反编译你的apk，我们还需要使用其他方法来防止apk被破解：

- 代码混淆技术，ProGuard提供了压缩，混淆，优化Java代码和（Shrinking），混淆（Obfuscation），优化（Optimition）Java代码和反混淆栈跟踪（ReTrace）的功能。
- NDK保护：逆向NDK程序的汇编代码比逆向Java代码枯燥和困难很多，同时使用C++也可以对敏感字符串和代码进行加密。
- 外壳保护：针对NDK编写的Native代码。

对抗动态调试

- 检测调试器：动态调试使用调试器来挂钩apk，获取apk运行时的数据，因此，我们可以在apk中加入检测调试器的代码，当检测到apk被调试器连接时，终止apk的运行。
- 检测模拟器：apk发布后，如果发现其运行在模拟器中，很有可能是有人试图破解或者分析它，因此这时我们也要终止apk的运行。

防止重编译

- 检查APK的签名
- 校验APK的完整性
- 校验classes.dex文件的完整性

参考资料

文末摄影鉴赏


ASCE1885
QQ: 380283392