<<Android软件安全与逆向分析>>

图书基本信息

书名：<<Android软件安全与逆向分析>>

13位ISBN编号：9787115308153

10位ISBN编号：7115308152

出版时间：2013-2

出版时间：人民邮电出版社

作者：丰生强

<<Android软件安全与逆向分析>>

内容概要

本书由浅入深、循序渐进地讲解了Android 系统的软件安全、逆向分析与加密解密技术。
包括Android软件逆向分析和系统安全方面的必备知识及概念、如何静态分析Android 软件、如何动态调试Android 软件、Android 软件的破解与反破解技术的探讨，以及对典型Android 病毒的全面剖析。

本书适合所有Android 应用开发者、Android 系统开发工程师、Android 系统安全工作者阅读学习。

作者简介

丰生强（网名非虫）Android软件安全专家。
看雪论坛Android安全版版主；安卓巴士开发交流版版主。
对Android软件与系统安全有狂热的爱好和独到的见解，对Android系统的全部源代码进行过深入地研究和分析。
逆向分析实战经验丰富。
在国内信息安全杂志上发表过多篇有价值的软件安全文章，目前就职于国内某Android开发企业，常年混迹于看雪论坛（ID非虫）。

<<Android软件安全与逆向分析>>

书籍目录

第1章Android程序分析环境搭建 1.1Windows分析环境搭建 1.1.1安装JDK 1.1.2安装Android SDK 1.1.3安装Android NDK 1.1.4Eclipse集成开发环境 1.1.5安装CDT、ADT插件 1.1.6创建Android Virtual Device 1.1.7使用到的工具 1.2Linux分析环境搭建 1.2.1本书的Linux环境 1.2.2安装JDK 1.2.3在Ubuntu上安装Android SDK 1.2.4在Ubuntu上安装Android NDK 1.2.5在Ubuntu上安装Eclipse集成开发环境 1.2.6在Ubuntu上安装CDT、ADT插件 1.2.7创建Android Virtual Device 1.2.8使用到的工具 1.3本章小结 第2章如何分析Android程序 2.1编写第一个Android程序 2.1.1使用Eclipse创建Android工程 2.1.2编译生成APK文件 2.2破解第一个程序 2.2.1如何动手？
2.2.2反编译APK文件 2.2.3分析APK文件 2.2.4修改Smali文件代码 2.2.5重新编译APK文件并签名 2.2.6安装测试 2.3本章小结 第3章进入Android Dalvik虚拟机 3.1Dalvik虚拟机的特点——掌握Android程序的运行原理 3.1.1Dalvik虚拟机概述 3.1.2Dalvik虚拟机与Java虚拟机的区别 3.1.3Dalvik虚拟机是如何执行程序的 3.1.4关于Dalvik虚拟机JIT（即时编译） 3.2Dalvik汇编语言基础为分析Android程序做准备 3.2.1Dalvik指令格式 3.2.2DEX文件反汇编工具 3.2.3了解Dalvik寄存器 3.2.4两种不同的寄存器表示方法——v命名法与p命名法 3.2.5Dalvik字节码的类型、方法与字段表示方法 3.3Dalvik指令集 3.3.1指令特点 3.3.2空操作指令 3.3.3数据操作指令 3.3.4返回指令 3.3.5数据定义指令 3.3.6锁指令 3.3.7实例操作指令 3.3.8数组操作指令 3.3.9异常指令 3.3.10跳转指令 3.3.11比较指令 3.3.12字段操作指令 3.3.13方法调用指令 3.3.14数据转换指令 3.3.15数据运算指令 3.4Dalvik指令集练习——写一个Dalvik版的Hello World 3.4.1编写smali文件 3.4.2编译smali文件 3.4.3测试运行 3.5本章小结 第4章Android可执行文件 4.1Android程序的生成步骤 4.2Android程序的安装流程 4.3dex文件格式 4.3.1dex文件中的数据结构 4.3.2dex文件整体结构 4.3.3dex文件结构分析 4.4odex文件格式 4.4.1如何生成odex文件 4.4.2odex文件整体结构 4.4.3odex文件结构分析 4.5dex文件的验证与优化工具dexopt的工作过程 4.6Android应用程序另类破解方法 4.7本章小结 第5章静态分析Android程序 5.1什么是静态分析 5.2快速定位Android程序的关键代码 5.2.1反编译apk程序 5.2.2程序的主Activity 5.2.3需重点关注的Application类 5.2.4如何定位关键代码——六种方法 5.3smali文件格式 5.4Android程序中的类 5.4.1内部类 5.4.2监听器 5.4.3注解类 5.4.4自动生成的类 5.5阅读反编译的smali代码 5.5.1循环语句 5.5.2switch分支语句 5.5.3try/catch语句 5.6使用IDA Pro静态分析Android程序 5.6.1IDA Pro对Android的支持 5.6.2如何操作 5.6.3定位关键代码——使用IDA Pro进行破解的实例 5.7恶意软件分析工具包——Androguard 5.7.1Androguard的安装与配置 5.7.2Androguard的使用方法 5.7.3使用Androguard配合Gephi进行静态分析 5.7.4使用androlyze.py进行静态分析 5.8其他静态分析工具 5.9阅读反编译的Java代码 5.9.1使用dex2jar生成jar文件 5.9.2使用jd—gui查看jar文件的源码 5.10集成分析环境——santoku 5.11本章小结 第6章基于Android的ARM汇编语言基础——逆向原生！
6.1Android与ARM处理器 6.1.1ARM处理器架构概述 6.1.2ARM处理器家族 6.1.3Android支持的处理器架构 6.2原生程序与ARM汇编语言——逆向你的原生Hello ARM 6.2.1原生程序逆向初步 6.2.2原生程序的生成过程 6.2.3必须了解的ARM知识 6.3ARM汇编语言程序结构 6.3.1完整的ARM汇编程序 6.3.2处理器架构定义 6.3.3段定义 6.3.4注释与标号 6.3.5汇编器指令 6.3.6子程序与参数传递 6.4ARM处理器寻址方式 6.4.1立即寻址 6.4.2寄存器寻址 6.4.3寄存器移位寻址 6.4.4寄存器间接寻址 6.4.5基址寻址 6.4.6多寄存器寻址 6.4.7堆栈寻址 6.4.8块拷贝寻址 6.4.9相对寻址 6.5ARM与Thumb指令集 6.5.1指令格式 6.5.2跳转指令 6.5.3存储器访问指令 6.5.4数据处理指令 6.5.5其他指令 6.6用于多媒体编程与浮点计算的NEON与VFP指令集 6.7本章小结 …… 第7章Android NDK程序逆向分析 第8章动态调试Android程序 第9章Android软件的破解技术 第10章Android程序的反破解技术 第11章Android系统攻击与防范 第12章DroidKongFu变种病毒实例分析

章节摘录

版权页： 插图： Android NDK的platforms＼〈android版本〉＼arch—arm＼usr＼include＼jni.h头文件中，声明了所有可以使用到的JNI接口函数。
该文件中有两个重要的结构体JNINativeInterface与JNIInvokeInterface，JNINativeInterface是JNI本地接口，实际上它是一个接口函数指针表，里面每一项都为JNI接口的函数指针，所有的原生代码都可以调用这些接口函数；而JNIInvokeInterface则是JNI调用接口，该结构目前只有3个保留项与5个函数指针，这5个函数用于访问全局的JNI接口，多用于原生多线程程序开发。
既然JNI为开发人员提供的API就在这两个接口内，那么掌握了这些API的含义与使用方法是不是就可以理解为掌握了Android NDK开发了呢？
笔者认为大多数时候是这样的。

编辑推荐

国内第一本Android软件安全书别让你的代码成为别人的炮灰eoe全球最大中文Android开发者社区、看雪论坛、安卓巴士　　推荐每一位Android开发者的必备之书！
在Android这个平台，我们已面临诸多威胁！
2013年超过1800万台Android设备会遭遇某种形式的恶意软件的攻击。
恶意代码和病毒数量呈指数增长； 应用软件和数字内容的版权不断遭到侵害； 软件破解、篡改、广告库修改和植入、应用内付费破解等普遍存在； 软件本身的安全漏洞也频繁出现在国内外互联网企业的产品中； 数据泄露和账户被盗等潜在风险让人担忧； 官方系统、第三方定制系统和预装软件的漏洞不断被发现。
要掌握主动，免除威胁，你应了解真相！
安全技术几乎都是双刃剑，它们既能协助我们开发更有效的保护技术，也几乎必定会被攻击者学习和参考。
这里的问题是，大量安全技术的首次大范围公开，是否会带来广泛的模仿和学习，从而引发更多的攻击？
在这个问题上，安全界一直存在争议。
这是任何一本里程碑式的安全书籍都无法绕开的话题。
在《信息安全工程》中，Ross Anderson说："尽管一些恶意分子会从这样的书中获益，但他们大都已经知道了这些技巧，而好人们获得的收益会多得多。
"正是基于对这种观念的认同，才使得这本书呈现于此。
强实践性。
这本书的几乎每一个部分，都结合实际例子，一步步讲解如何操作。
缺乏可操作性，是Android安全方面现有论文、白皮书、技术文章最大的问题之一，很多人读到最后可能对内容有了一些概念，却不知道从何下手。
强时效性。
作者在写作的同时，持续跟随业界最新进展，刚刚发布不久的Santoku虚拟机、APIMonitor等工具，以及Androguard的新特性等，已然出现在了这本书中。

版权说明