Android 软件安全攻防实例分析

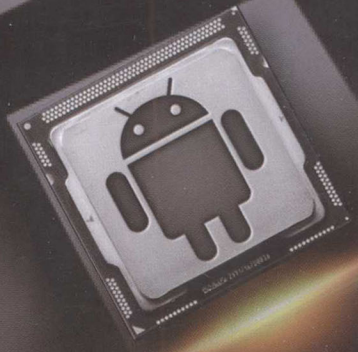
徐君锋　张 利◎主编

国内首部Android软件安全实战书籍

逾30款热点软件攻防对抗案例剖析

顺藤摸瓜多角度破解典型游戏软件

庖丁解牛追踪恶意代码的蛛丝马迹



科学出版社

Android 软件安全攻防实例分析

徐君锋　张利　主编

科学出版社
北京

内 容 简 介

本书源自当前流行的各种 Android 主流软件，特别是 Android 有代表性的游戏软件破解实例，针对 Android 软件安全的主流攻防技术，详细记录破解和反破解 Android 软件的过程，深度分析攻防技术细节，从不同侧面描述 Android 软件攻防的技术内容，寄希望于相关管理和技术人员从这些实例和技术中得到启示，高度重视 Android 软件安全，并得到有价值的技术借鉴，或者从中学到有用的技术。

本书可供 Android 软件逆向工程和攻防技术的初学者、自学者和爱好者阅读参考，也可作为 Android 安全专业人员的参考书。

图书在版编目（CIP）数据

Android软件安全攻防实例分析/徐君锋，张利主编. — 北京：科学出版社，2017.2

ISBN 978-7-03-050381-7

Ⅰ. A… Ⅱ. ①徐… ②张… Ⅲ. 移动终端-应用程序-程序设计-安全技术 Ⅳ. ①TN929.53

中国版本图书馆CIP数据核字（2016）第261930号

责任编辑：杨 凯 / 责任制作：魏 谨
责任印制：张 倩 / 封面设计：杨安安
北京东方科龙图文有限公司 制作
http://www.okbook.com.cn

科学出版社出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

三河市骏杰印刷有限公司 印刷
科学出版社发行 各地新华书店经销

*

2017年2月第 一 版 开本：720×1000 1/16
2017年2月第一次印刷 印张：23
字数：465 000

定价：58.00元

（如有印装质量问题，我社负责调换）

前 言

目前，移动互联网已经成为一股势不可当的力量，急剧而深刻地影响并改变着人们的生产和生活方式。在移动互联网操作系统中，Android 名列前茅，其全球市场占有率在 2016 年第一季度已经达到 86.2%。然而，由于 Android 系统的开放性，非法黑客通过逆向工程和反编译等技术手段，可以随意将大量的时下流行的软件或者游戏进行反编译，再植入扣费代码后再重新封装软件包，最后在各大第三方 Android 市场及论坛上被随意发布。同时，恶意攻击者也能够利用 Android 手机漏洞窃取敏感的用户信息，通过短信拦截等方式疯狂敛财或创建僵尸网络。据中国互联网协会和国家互联网应急中心联合发布的《中国移动互联网发展状况及其安全报告 (2016)》称，2016 年感染移动互联网恶意程序的我国境内用户高达 1.94 亿。Public Intelligence 网站公布的数据表明有 79% 的恶意软件针对 Android 系统。因此，Android 系统平台俨然成为网络空间恶意病毒的重灾区，Android 软件的安全问题已经危及个人隐私安全、财产安全甚至国家信息安全。例如，CCTV 隔三差五都会报道某人又因手机恶意短信被诈骗若干万元，某省警方又从某国抓获使用手机短信的电信诈骗犯罪团伙等，就连广场舞大妈都知道使用某破解软件去除 Android 手机里面某音乐软件的注册码，吃瓜群众也明白为自己的 Android 手机安全装上最新版本的杀毒软件。同时，市面上关于 Android 安全的书籍和资料真所谓五花八门，让人眼花缭乱。为了有效防范 Android 手机的金融诈骗、非法信息获取等犯罪活动，了解不法分子对 Android 软件的修改模式、破解手段、渗透方法、攻击途径、加固策略等攻防技术显得尤为重要。

然而，对于刚接触 Android 软件安全的爱好者来说，如果没有实践练习，会因为枯燥的理论学习知难而退或感觉索然无味；就算是 Android 软件安全从业者，缺少了必要的实践支撑，其专业知识结构也会显得苍白和空洞。从实践中来，到实践中去，学之根本，习之标榜。所以在本书中，作者力求去除繁琐的理论叙述，开门见山通过实践案例，从一个叙述者角度同读者交谈，甚至使用一些非专业化语言，剖析相关专业技术细节，

解说 Android 软件攻防实战过程。

本书共九章，从 Android 软件攻防的基础知识到高级技术，由简入繁，循序渐进。

第 1 章介绍 Android 软件开发和逆向工程工作环境搭建过程和配置，介绍主流 Android 逆向工程工具的特点和简单使用方法，旨在让读者快速入门。

第 2 章简略介绍 Android 逆向工程必备的基础知识，包括 APK 文件、smali 语言、Dex 文件、ELF 格式、ARM 汇编等。

第 3 章从 Android 逆向工程数据包中抽取各类资源文件入手，在 XML、smali 和 so 文件中直接修改 Android 软件资源，实现界面修改、汉化、程序捆绑等功能。

第 4、5 章分别从软件静态分析和动态分析的角度，列举分析了如何破解和去除 APK 程序的使用限制技术和方法。

第 6 章从 Android 软件攻防两个角度分析了国内 BAT3、梆梆、爱加密等安全公司加固的软件脱壳和安全防护技术。

第 7 章内容相对繁杂，介绍复杂网络环境下 Android 软件安全的分析技术，特别是网络抓包分析、Root、复杂密码解密等。

第 8 章从技术的角度深度分析了当前几款 Android 木马病毒，这是 Android 逆向工程较为高级的阶段。

第 9 章撇开软件通用的代码混淆和校验等防护技术，从模拟器检测和函数加密的方式介绍 Android 软件攻击安全风险防范的策略和方法。

佛家有云：“世间万物皆是相生相克、相互制衡。”可谓“魔高一尺道高一丈”，Android 软件安全攻防技术的博弈在一场无休止的战役中此消彼长，双方时而对抗厮杀，争斗情势你死我活，时而齐头并进，比翼双飞。Android 软件静态渗透攻击手段会有静态加固策略用以防范，而 Android 软件动态加固技术总会出现新的动态破解和跟踪的方法进行对抗。一个 Android 漏洞被爆出，很快就会发布修复补丁，而不久以后又会爆出更新的 Android 漏洞。在 Android 软件安全攻防技术这场永无止息的战斗中，考验双方的只是时间。

孙子兵法曰：“知己知彼，百战不殆。”本书的终极目标并非仅仅传播技术，而是既希望专业读者能够在洞悉技术的基础上增强 Android 软件安全性，造福用户；也希望初级读者能够足够重视自身的设备安全，学会自我保护。要知道，手握 Android 软件攻

防技术这把双刃剑的指挥者是人而非剑。

最后作者诚挚感谢对本书提供技术支撑的业内大牛们，他们来自360、腾讯、阿里、百度等国内知名安全公司，主要有（排名不分先后）丰生强（非虫）、周烨（鬼哥）、杨付伟（我是小三）、宋煜禧（人生无NG）、万园春（万抽抽）、何垚（小雨）、王勇（THOMASKING）、林岳川（Z_zAge）、贾志军（Jack-jia）等同仁。

同时，本书得到国家自然科学基金面上项目“基于动态加固的Android软件安全保护建模方法与决策控制研究（批准号：61672534）”和国家自然科学基金重点项目“网络大数据中的跨媒体并发隐信道的检测与对抗方法（批准号：U1536207）”的支持。

由于作者水平有限，加之时间仓促，书中错误和不当之处在所难免，敬请读者和同行专家批评指正！本书涉及的软件攻防实例仅从技术角度解读，作者不提供任何软件样本，请读者在遵守我国相关法律的前提下阅读和使用。

目 录

第1章 工欲善其事必先利其器：Android软件逆向工程工作环境

1.1 部署Android开发与逆向工程工作环境

Android逆向工程技术是建立在熟练掌握Android开发技术的基础上的，所以建立Android开发环境也是Android逆向工作的开端。Android逆向工作可以在各种操作系统下进行，包括Windows、Linux、iOS，甚至是Android系统本身。本书以Windows环境为例部署工作环境，在其他操作系统下部署工作大同小异。

准备文件如图1.1所示，下载地址及步骤如下：

（1）下载Android SDK：http://developer.android.com/sdk/index.html，Windows 7的安装方法与Windows XP的安装方式完全相同。

（2）下载JDK8：http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html。

（3）下载Eclipse Neon：https://www.eclipse.org/downloads/download.php?file=/oomph/epp/neon/R/eclipse-inst-win64.exe。

（4）下载Eclipse的Android ADT插件。许多教程在这一步都是通过Eclipse自身的update功能进行下载：启动Eclipse，选择“Help”->“Soft Updates”>“Find and Install…”。这里，我们选择“Available Software”标签页，点击“Add Site…”按键，添加update站点：https://dl-ssl.google.com/android/eclipse/。这时窗口中新增了“https://dl-ssl.google.com/android/eclipse/”项，选中该项，点击“Install…”按键即可下载。

【注意】许多国内的用户都无法完成这样的升级，通常是进行到一半就没有任何反映了（其他插件，例如pydev也是这样）。这样，我们直接到Android官网去下载这个ADT插件：https://dl.google.com/android/ADT-23.0.7.zip。下载完成后，按如下步骤安装：Help->Install New Software…->Add…->Archive选

择 zip 文件 ->OK。

名称	修改日期	大小
ADT-23.0.7.zip	2015/12/14 14:44	100,934 KB
Android_sdk_installer_r24.4.1.exe	2016/7/15 10:43	148,106 KB
eclipse-inst-win64.exe	2016/7/15 11:03	45,854 KB
jdk-8u66-windows-x64.exe	2015/12/11 13:09	191,135 KB

图 1.1　准备文件

安装配置过程如下：

1. **安装 JDK**

运行 jdk-8u66-windows-x64.exe，如图 1.2 所示。

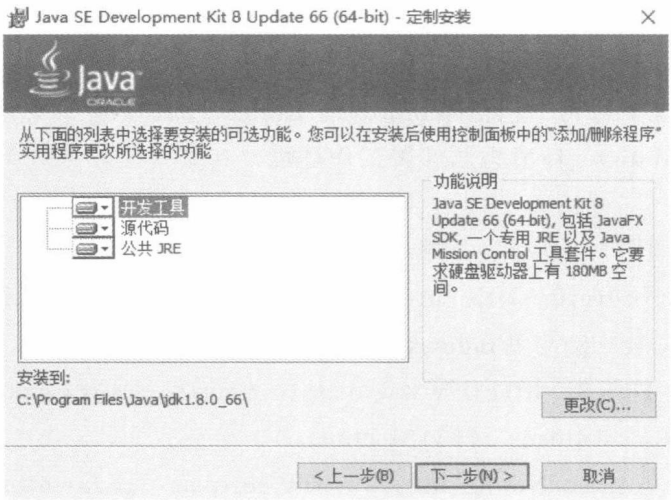


图 1.2

检查 JDK 是否安装成功。如图 1.3 所示，打开 cmd 窗口，输入 java-version 查看 JDK 的版本信息。

图 1.3

2. 安装 Eclipse

运行 eclipse-inst-win64.exe，选择所需版本的 Eclipse，如图 1.4 所示。

图 1.4

运行 eclipse.exe，设置 Workspace，指定一个开发目录给它就可以了（图 1.5）。

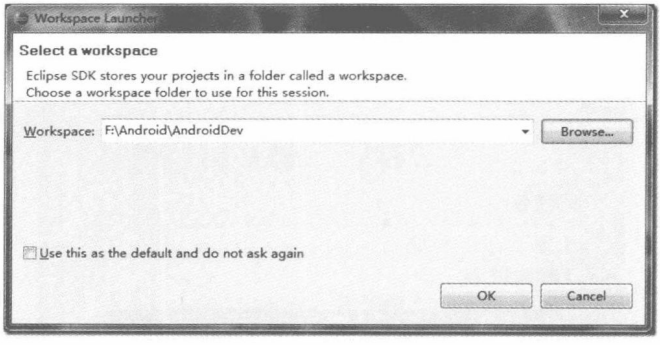


图 1.5

至此，Eclipse 安装完毕。

3. 安装 Android sdk

运行 Android_sdk_installer_r24.4.1.exe，如图 1.6 所示。

图 1.6

将 Android SDK 中的 tools 绝对路径添加到系统 PATH 中。打开“系统属性”选择“环境变量”，添加环境变量 PATH 值为 SDK 中 tools 的绝对路径，如图 1.7 所示。

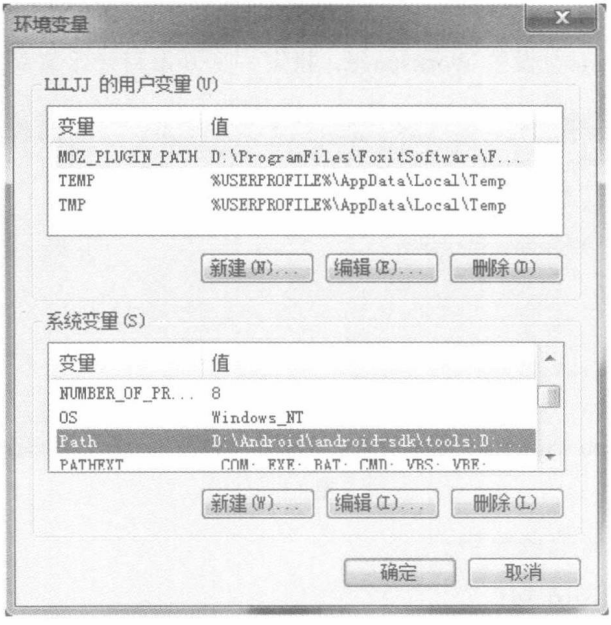


图 1.7

点击“确定”后，重新启动计算机。

重启计算机以后，进入 cmd 命令窗口，检查 SDK 是否安装成功。

运行 android –h，如果输出图 1.8 所示内容，表明安装成功。

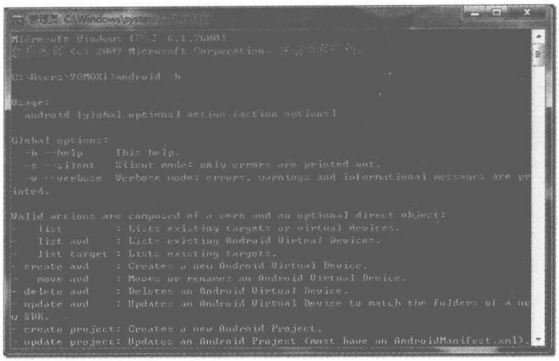


图 1.8

4. **安装 Android Development Tools（ADT）**

打开 Eclipse IDE，进入菜单中的“Help”–> “Software Updates”（图 1.9）。

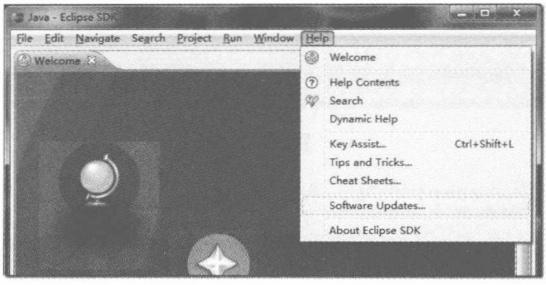


图 1.9

如图 1.10 所示，进入选项卡“Available Software”–> “Add Site”–> “Location:”，输入 http://dl-ssl.google.com/android/eclipse。

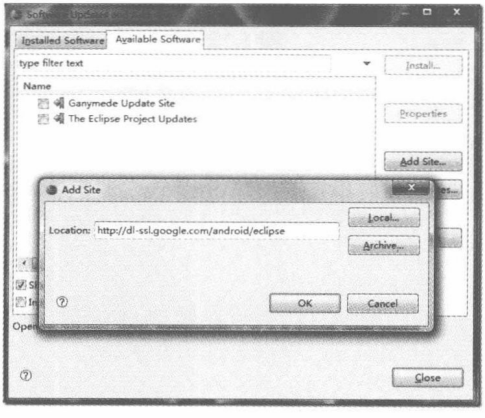


图 1.10

勾选“Android DDMS”和“Android Development Tools”，“Install”如图 1.11 所示。

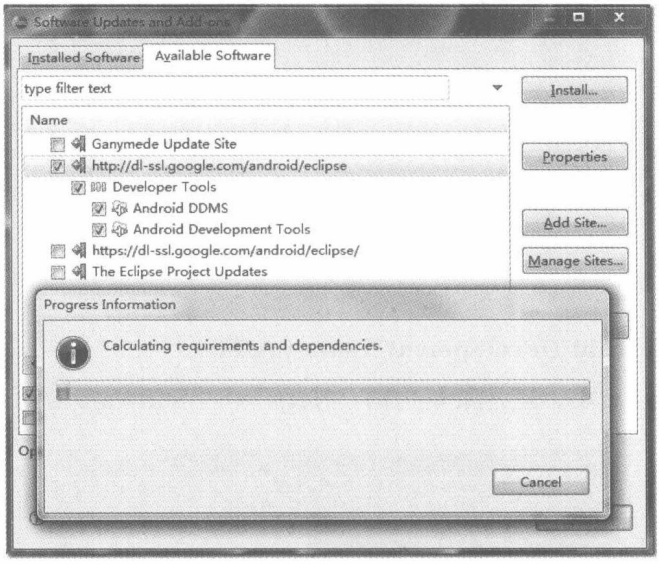


图 1.11

一直 Next，注意 Accept 许可，直到完成。

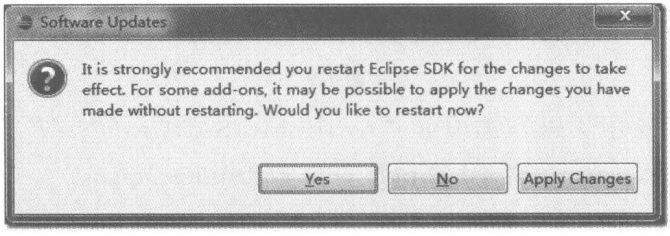


图 1.12

点击“Yes”，然后重启“Eclipse”，完成安装。

5. 设定“SDK Location”

打开 Eclipse IDE，进入菜单中的“Window”–>“Preferences”，如图 1.13 所示。

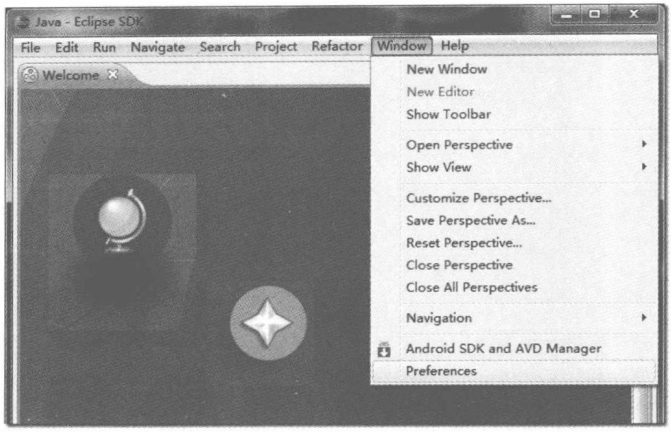


图 1.13

打开“Preferences”窗口，选中“Android”，直接设定“SDK Location”为 SDK 的安装目录（图 1.14）。

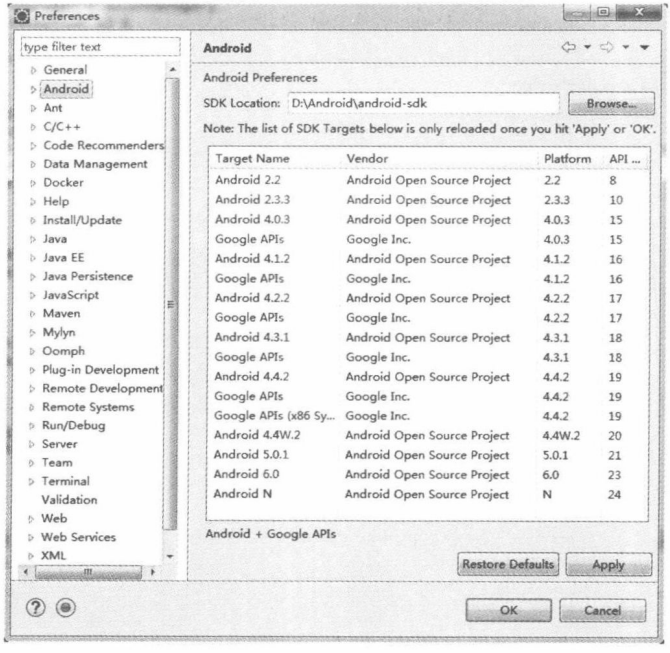


图 1.14

6. 验证开发环境，并创建 HelloWorld 测试程序

如图 1.15 所示，进入 Eclipse IDE 菜单中的“File” -> “New” -> “Android Application Project”。

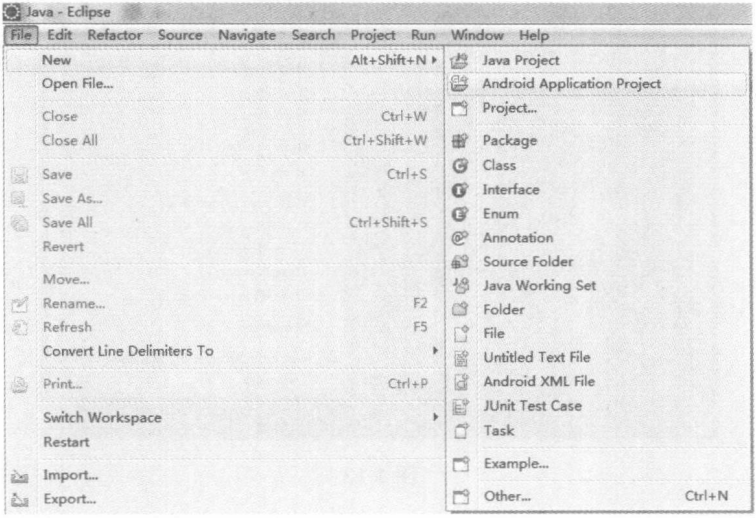


图 1.15

参考图 1.16，完成基本信息的配置。

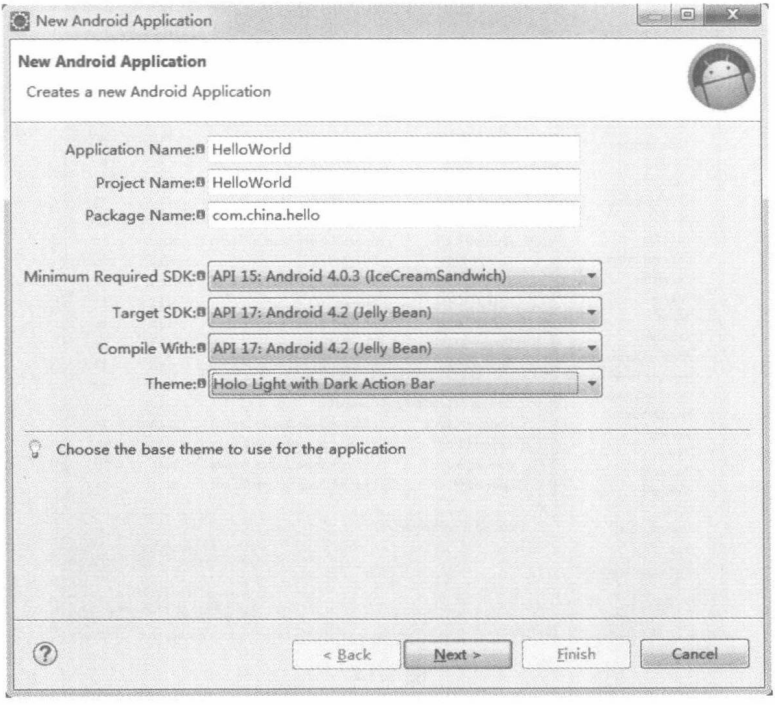


图 1.16

其他项目按缺省配置，直到最后一步，将“Activity Name”命名为 HelloChina，点击“Finish”完成工程创建（图 1.17）。