TURING 图灵程序设计丛书

[PACKT] PUBLISHING

【印】Srinivasa Rao Kotipalli Mohammed A. Imran 著 李骏 译

Android 安全攻防实践

Hacking Android

从实验环境搭建开始一步步指导你掌握Android安全攻防技能
全面深入研究安卓系统，使设备免受安全威胁

中国工信出版集团 人民邮电出版社 POSTS & TELECOM PRESS

Android 安全攻防实战

Hacking Android

TURING 图灵程序设计丛书

Hacking Android

Android 安全攻防实践

[印] Srinivasa Rao Kotipalli Mohammed A. Imran 著

李骏 译

人民邮电出版社

北 京

图书在版编目（CIP）数据

Android安全攻防实践 / (印) 斯里尼瓦沙·拉奥·科提帕里, (印) 穆罕默德·阿·伊姆兰著 ; 李骏译. -- 北京 : 人民邮电出版社, 2018.4
（图灵程序设计丛书）
ISBN 978-7-115-48026-2

Ⅰ. ①A… Ⅱ. ①斯… ②穆… ③李… Ⅲ. ①移动终端－应用程序－程序设计 Ⅳ. ①TN929.53

中国版本图书馆CIP数据核字(2018)第043990号

内 容 提 要

本书以搭建安卓安全所需的实验环境开篇，首先介绍了ROOT安卓设备的常用工具和技术，并分析了安卓应用的基本架构，接着从数据存储、服务器端、客户端等方面讲解了安卓应用可能面临的安全风险；最后给出了一些避免恶意攻击的方法。另外，本书还涉及了多个案例，步骤详实，通俗易懂。

本书适合想了解安卓安全的读者、移动开发人员、软件工程师和QA专家等。

◆ 著　[印] Srinivasa Rao Kotipalli　Mohammed A. Imran
译　李　骏
责任编辑　朱　巍
执行编辑　潘明月
责任印制　周昇亮

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路11号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市潮河印业有限公司印刷

◆ 开本：800×1000　1/16
印张：16.75
字数：390千字　2018年4月第1版
印数：1－3 000册　2018年4月河北第1次印刷
著作权合同登记号　图字：01-2017-9036号

定价：59.00元

读者服务热线：(010)51095186转600　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

站在巨人的肩上

Standing on Shoulders of Giants

iTuring.cn

前　言

移动安全是当下最热门的话题之一。作为市场上领先的移动操作系统，安卓拥有极其广泛的用户基础，大量的个人数据和商业数据都存储在安卓移动设备上。移动设备给人们带来了娱乐、商业、个人生活，同时也带来了新的风险，针对移动设备和移动应用的攻击日益增加。作为用户群最大的平台，安卓自然成为攻击者首选的攻击目标。本书将深入研究各种攻击技术，以便帮助开发人员、渗透测试人员以及终端用户了解安卓安全的基本原理。

内容概述

第1章“实验环境搭建”是本书的基础部分。这一章将会指导读者搭建一个环境，其中囊括了后面各章所需的所有工具。对于不了解安卓安全技术的读者来说，这一章属于基础入门部分，将指导他们安装安卓安全所需的一系列工具。

第2章“安卓ROOT”介绍ROOT安卓设备的常见技术。这一章将介绍ROOT的基础知识，并分析其利弊，之后讨论安卓的分区布局、boot loader 以及boot loader解锁技术等话题。这一章将指导读者如何ROOT自己的设备，并了解ROOT概念的来龙去脉。

第3章“安卓应用的基本构造”概述安卓应用的内部构造。应用在底层是如何构造的，当它们被安装到设备上时是什么样子，又是如何运行的，等等，了解这些知识非常有必要，而这也正是这一章所涵盖的内容。

第4章“安卓应用攻击概览”概述安卓的攻击面。这一章将讨论安卓应用、安卓设备以及安卓应用结构体系中其他组件可能遭受的攻击。更重要的是，指导读者针对通过网络与数据库通信的传统应用构建一个简易威胁模型。了解应用可能遭受的攻击对于理解渗透测试的测试内容十分重要。这一章对上述内容进行了高度概括，只包含少量技术细节。

第5章“数据存储与数据安全”介绍评估安卓应用数据存储安全的常见技术。数据存储是安卓应用开发中最重要的部分之一。这一章将首先讨论开发者在本地存储数据时所使用的不同技术，以及这些技术对安全性的影响。然后，具体阐述开发者所选用的数据存储技术对安全性的影响。

第6章“服务器端攻击”概述在服务器端安卓应用的攻击面。这一章将高度概括安卓应用后端可能遭受的攻击，并包含了少量的技术细节，因为大部分服务器端漏洞都与Web攻击有关。OWASP测试和开发者指南已经详细介绍了Web攻击。

第7章“客户端攻击——静态分析技术”从静态应用安全测试（SAST）的角度介绍各种客户端攻击。静态分析是一种通过可轻易获得的安卓逆向工具来鉴别安卓应用漏洞的通用技术。这一章还将讨论一些用于对安卓应用进行静态分析的自动化测试工具。

第8章“客户端攻击——动态分析技术”将介绍动态应用安全测试（DAST）中用于评估和利用安卓应用客户端漏洞的一些常用工具和技术。另外，还会讨论Xposed、Frida等在运行时操控应用的工具。

第9章“安卓恶意软件”将介绍创建和分析安卓恶意软件的常用基础技术。这一章将首先介绍传统安卓恶意软件的特征，然后讨论如何创建一个简单的恶意软件，并用于在受感染的手机上给攻击者一个反弹shell。最后讨论安卓恶意软件的分析技术。

第10章“针对安卓设备的攻击”试图帮助用户在日常使用中免受攻击，譬如在咖啡店和机场连接免费Wi-Fi时，如何免受攻击。这一章还将解释为什么ROOT安卓设备和安装未知来源的应用是不安全的。

阅读准备

为了在阅读本书的同时能亲自体验，读者需要安装下列软件。下载链接和安装步骤将在后面说明。

- Android Studio
- 安卓模拟器
- Burp Suite
- Apktool
- Dex2jar
- JD-GUI
- Drozer
- GoatDroid
- QARK
- Cydia Substrate
- Introspy
- Xposed框架
- Frida

读者对象

本书适合想了解安卓安全的读者，对软件工程师、QA专业人员、初级及中级安全专业人士都有帮助。如果有一些安卓编程基础更佳。

排版约定

在本书中，你会看到一些不同的文本样式，用以区分不同类型的信息。下面举例说明一些样式的具体含义。

文中的代码、数据库表名、用户输入等将使用如下样式："内容提供程序使用标准的`insert()`、`query()`、`update()`和`delete()`等方法来获取应用数据。"

代码段的格式如下：

```
@Override
public void onReceivedSslError(WebView view, SslErrorHandler handler,
SslError error)
{
   handler.proceed();
}
```

代码段中需要重点关注的部分将会加粗：

```
if(!URL.startsWith("file:")) {
```

命令行输入和输出格式如下：

```
$ adb forward tcp:27042 tcp:27042
$ adb forward tcp:27043 tcp:27043
```

此图标表示警告或重要提示。

此图标表示提示和技巧。

读者反馈

我们非常欢迎读者的反馈。让我们知道你对本书的想法——喜欢哪些部分，或不喜欢哪些部分。你的反馈将会帮助我们开发能够真正被大家充分利用的图书。

你可以发送邮件到feedback@packtpub.com进行反馈，并在邮件主题中注明书名。

如果你对某一个主题有专业的见解，而且有兴趣创作或者为一本书做出贡献，请参考我们在www.packtpub.com/authors上的作者指南。

用户支持及说明

我们将为本书的读者提供最大的帮助，使读者能从本书中获得最大的收获。本书旨在深入研究各种攻击技术，任何未经所有者许可而攻击其系统的做法均属非法行为。

下载示例代码

读者可以通过账号从http://www.packtpub.com下载示例代码。如果你是从别处购买的本书，则可以访问http://www.packtpub.com/support，并注册账号，所有文件将会通过邮件直接发送给你。

可以按照下面的步骤下载代码文件：

(1) 使用你的邮箱和邮箱密码登录我们的网站或者注册账号；
(2) 将鼠标移动到网站顶部的SUPPORT选项卡；
(3) 点击Code Downloads & Errata；
(4) 在搜索框输入书名；
(5) 选中你要下载代码文件的图书；
(6) 在下拉菜单中选择购买渠道；
(7) 点击Code Download。

也可以访问本书在Packt出版社官方网站的页面，点击网页上的Code Files按钮进行下载。你可以通过在搜索框中输入书名找到该页面。注意，你要登录Packt账号才能下载。

文件下载完成后，使用下列软件的最新版将下载的文件解压或导出。

- Windows平台：WinRAR/7-Zip
- Mac平台：Zipeg/iZip/UnRarX
- Linux平台：7-Zip/PeaZip

我们也在GitHub上托管了本书的代码：https://github.com/PacktPublishing/hacking-android。Packt图书和视频的代码也能在https://github.com/PacktPublishing/上找到。赶紧前往查看吧！

勘误表

尽管我们尽了最大的努力来保证书中内容的准确性，但差错还是在所难免。如果你发现了书中的错误，不论是正文还是代码，并且能够反馈给我们，我们将十分感激。这么做不仅能解决其

他读者的困惑，也能帮助我们在本书后续版本中进行改进。如果你发现了错误，可以访问http://www.packtpub.com/submit-errata，选择相应的图书，点击Errata Submission Form链接，填写勘误详情。一旦勘误审核通过，你的提交将会被接受，并上传到我们的网站或者添加到现有勘误表中。

查看之前读者提交的勘误表，请访问https://www.packtpub.com/books/content/support，并在搜索框中输入书名查询。所需的信息将会显示在Errata下面。

盗版行为

对于所有媒体而言，网络盗版行为是一个长期存在的问题。对Packt而言，我们将严格保护自身的版权和许可证。如果你在网络上发现Packt作品的任何非法副本，请立即将网址或网站名称告诉我们，以便我们采取补救措施。

请将涉嫌盗版的链接通过邮件发送至copyright@packtpub.com。

感谢读者保护我们的作者，保护我们为读者提供有价值内容的能力。

读者提问

如果读者对于本书内容有任何疑问，可以通过邮箱questions@packtpub.com联系我们，我们将尽最大的努力帮助读者解决问题。

电子书

扫描如下二维码，即可购买本书电子版。

致　谢

Srinivasa Rao Kotipalli 的致谢

首先，我要感谢家人在我撰写本书的过程中给予我的支持和鼓励。没有他们的支持，也不会有本书。

衷心感谢我的好友 Sai Satish、Sarath Chandra、Abhijeth、Rahul Venati、Appanna K和Prathapareddy。他们从我职业生涯刚开始的时候就一直陪伴在我身边。

特别感谢 G.P.S. Varma博士、S.R.K.R.工程学院的院长、Sagi Maniraju先生、G. Narasimha Raju先生、B.V.D.S. Sekhar先生、S. Ram Gopal Reddy先生、Kishore Raju先生以及S.R.K.R.学院信息技术系的所有员工，感谢他们在我毕业期间给予我的支持和指导。

衷心感谢我的导师Prasad Badiganti，是他宝贵的建议和指导使我成为了一位真正的专家。

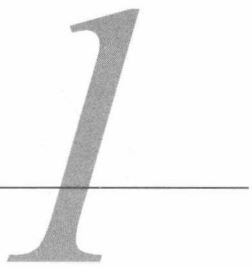
最后，感谢Packt出版社团队，特别是Divya、Trusha和Nirant，他们竭尽全力地帮助我们来保证本书的顺利出版。

Mohammed A. Imran 的致谢

首先，我要感谢父母这些年对我的关爱和支持。我还要感谢我美丽的妻子，她不仅给我的生活带来了欢乐，同时对我的业余项目也很有耐心。此外，还要感谢我的兄弟姐妹，Irfan、Fauzan、Sam和Sana，他们是我在这世界上最好的兄弟姐妹。

目　录

第 1 章 实验环境搭建



在本章中，我们将搭建一个实验环境，其中包含后续章节所需的各种工具。对于不了解安卓安全技术的读者来说，本章属于基础入门部分。它将指导我们安装所需的一系列安卓安全工具。

下面是本章将要讨论的主要内容。

- 设置安卓环境
- 安装应用评估所需的工具
- 安装评估移动设备后端安全所需的工具
- 安装易受攻击的应用
- Android Debug Bridge（adb）[①]介绍

1.1 安装工具

本节将介绍后续章节会用到的各种工具。首先，安装用于开发安卓应用的Android Studio；然后，创建一个安卓虚拟机（AVD）；最后，安装用于评估安卓应用和设备安全性的必要工具。本节介绍的大部分安装步骤都是针对Windows平台的，如果是针对其他平台的工具，会特别指出。

Java

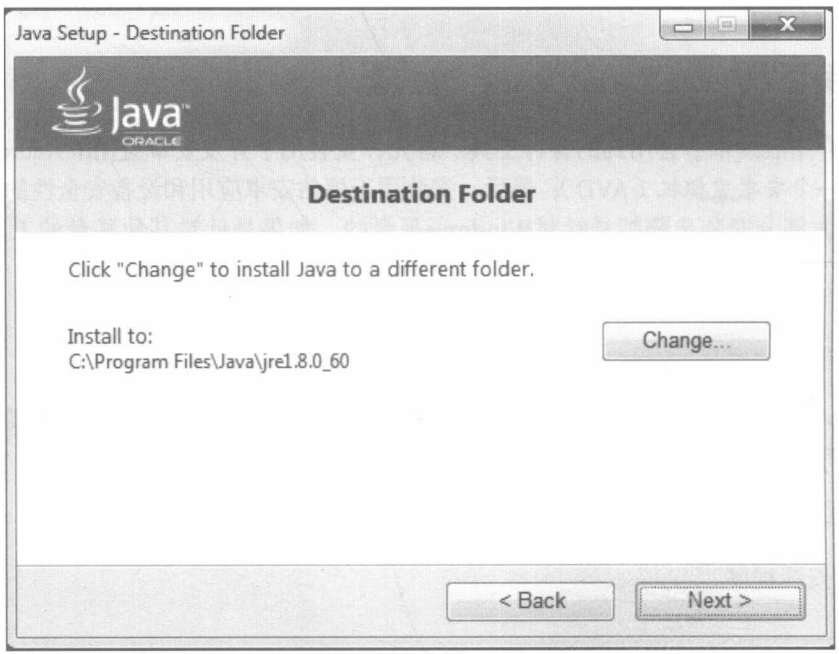
像Android Studio和Burp Suite这样的工具都离不开Java。因此，先从下面的链接下载并安装Java：https://java.com/zh_CN/download/。

下面是安装Java的步骤。

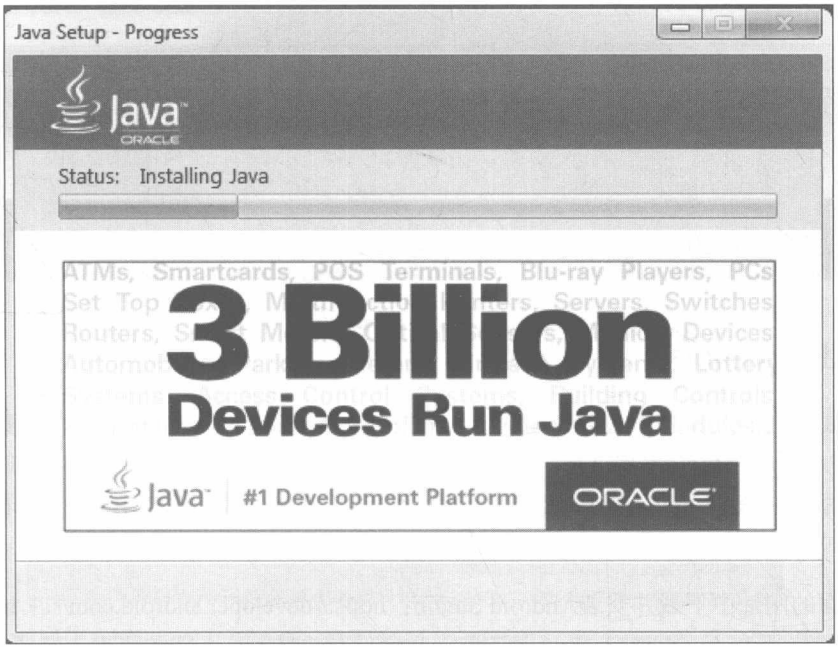
(1) 运行安装程序。

① 安卓操作系统与桌面计算机间沟通的一个命令行工具。——译者注

(2) 如果需要修改安装路径，勾选Change按钮，选择目标文件夹。否则，保留默认设置即可。点击Next按钮，会出现如下图所示的界面。



(3) 点击Next按钮，进入安装界面。



(4) 出现如下图所示的界面表示安装完成。