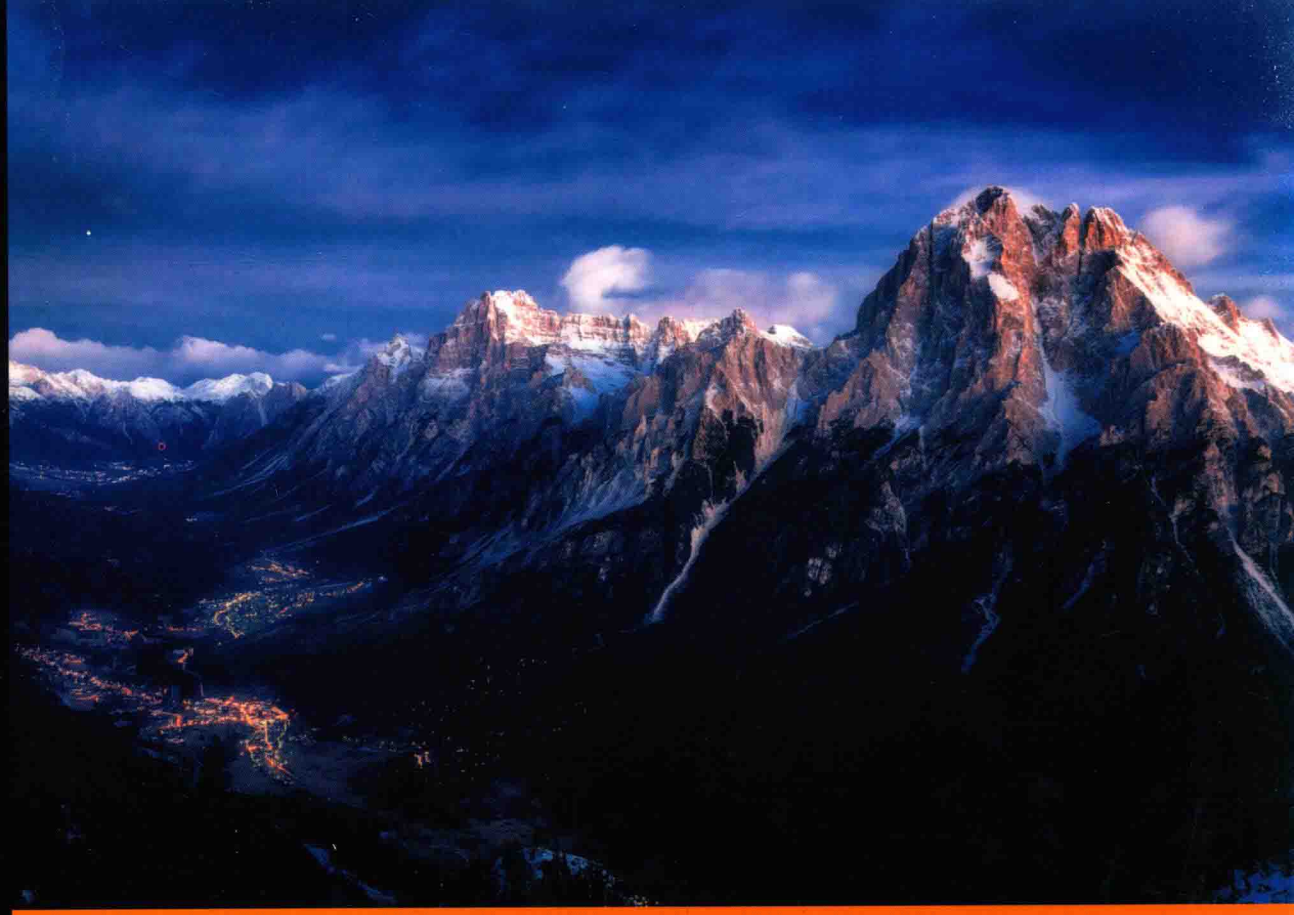

安卓黑客手册（影印版）

Hacking Android

Srinivasa Rao Kotipalli, Mohammed A. Imran 著

[PACKT] PUBLISHING

东南大学出版社 SOUTHEAST UNIVERSITY PRESS

安卓黑客手册(影印版)

Hacking Android

Srinivasa Rao Kotipalli, Mohammed A. Imran 著

南京　东南大学出版社

图书在版编目(CIP)数据

安卓黑客手册:英文/(印)司瑞妮瓦萨·R.孔提帕里(Srinivasa Rao Kotipalli),(新加坡)穆罕默德·A.伊姆兰(Mohammed A. Imran)著. —影印本. —南京:东南大学出版社,2017.10

书名原文:Hacking Android

ISBN 978-7-5641-7362-3

Ⅰ.①安… Ⅱ.①司… ②穆… Ⅲ.①移动电话机-操作系统-安全技术-手册-英文 Ⅳ.①TP929.53-62 ②TP316.85-62

中国版本图书馆 CIP 数据核字(2017)第 192636 号

图字:10-2017-116 号

安卓黑客手册(影印版)

出版发行:东南大学出版社
地　　址:南京四牌楼 2 号　　邮编:210096
出 版 人:江建中
网　　址:http://www.seupress.com
电子邮件:press@seupress.com
印　　刷:常州市武进第三印刷有限公司
开　　本:787 毫米×980 毫米　16 开本
印　　张:23.5
字　　数:460 千字
版　　次:2017 年 10 月第 1 版
印　　次:2017 年 10 月第 1 次印刷
书　　号:ISBN 978-7-5641-7362-3
定　　价:82.00 元

本社图书若有印装质量问题,请直接与营销部联系。电话(传真):025-83791830

Credits

Authors
Srinivasa Rao Kotipalli
Mohammed A. Imran

Reviewer
Guangwei Feng

Commissioning Editor
Edward Gordon

Acquisition Editor
Divya Poojari

Content Development Editor
Trusha Shriyan

Technical Editor
Nirant Carvalho

Copy Editors
Safis Editing
Madhusudan Uchil

Project Coordinator
Kinjal Bari

Proofreader
Safis Editing

Indexer
Hemangini Bari

Graphics
Kirk D'Penha

Production Coordinator
Arvindkumar Gupta

Cover Work
Arvindkumar Gupta

About the Authors

Srinivasa Rao Kotipalli (`@srini0x00`) is a security researcher from India. He has extensive hands-on experience in performing web application, infrastructure, and mobile security assessments. He worked as a security consultant at Tata Consultancy Services India for two and a half years and later joined a start-up in Malaysia. He has delivered training sessions on web, infrastructure, and mobile penetration testing for organizations across the world, in countries such as India, Malaysia, Brunei, and Vietnam. Through responsible disclosure programs, he has reported vulnerabilities in many top-notch organizations. He holds a bachelor's degree in information technology and is OSCP certified. He blogs at `www.androidpentesting.com` and `www.infosecinstitute.com`.

First and foremost I would like to thank my family members for their support and encouragement while writing this book. This would never have happened without their support.

Many thanks to my special friends Sai Satish, Sarath Chandra, Abhijeth, Rahul Venati, Appanna K, Prathapareddy for always being with me right from the beginning of my career.

Special thanks to Dr. G.P.S. Varma, principal of S.R.K.R Engineering College, Mr. Sagi Maniraju, Mr. G. Narasimha Raju, Mr. B.V.D.S Sekhar, Mr. S RamGopalReddy, Mr. Kishore Raju and all the staff members of S.R.K.R, Information Technology Department for their wonderful support and guidance during my graduation.

Huge thanks to Mr. Prasad Badiganti for being my mentor and tuning me into a true professional with his valuable suggestions.

Last but not the least, thanks to the Packt Publishing team especially Divya, Trusha & Nirant for helping us in every way possible to get this book to this stage.

Mohammed A. Imran (`@secfigo`) is an experienced application security engineer and the founder of null Singapore and null Hyderabad. With more than 6 years of experience in product security and consulting, he spends most of his time on penetration testing, vulnerability assessments, and source code reviews of web and mobile applications. He has helped telecom, banking, and software development houses create and maintain secure SDLC programs. He has also created and delivered training on application security and secure coding practices to students, enterprises, and government organizations. He holds a master's degree in computer science and is actively involved in the information security community and organizes meetups regularly.

First and foremost, I want to thank my parents for all their love and support during all these years. I want to thank my beautiful wife for bringing joy in my life and for being patient with all my side projects. I also want to thank my siblings Irfan, Fauzan, Sam and Sana for being the best siblings ever.

About the Reviewer

Guangwei Feng is a mobile developer at Douban (`https://www.douban.com/`) in Beijing. He holds a master's in information technology from University of Sydney and a BE from Nankai University (Tianjin). He is a part of the Douban app (social), Douban Dongxi app (online shopping), and TWS for Douban FM (wearable) projects. Out of these, the Douban app has been downloaded over 10 million times and has become one of the most popular apps in China.

www.PacktPub.com

eBooks, discount offers, and more

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.PacktPub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `customercare@packtpub.com` for more details.

At `www.PacktPub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

`https://www2.packtpub.com/books/subscription/packtlib`

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can search, access, and read Packt's entire library of books.

Why subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print, and bookmark content
- On demand and accessible via a web browser

Preface

Mobile security is one of the hottest topics today. Android being the leading mobile operating system in the market, it has a huge user base, and lots of personal as well as business data is being stored on Android mobile devices. Mobile devices are now sources of entertainment, business, personal life, and new risks. Attacks targeting mobile devices and apps are on the rise. Android, being the platform with the largest consumer base, is the obvious primary target for attackers. This book will provide insights into various attack techniques in order to help developers and penetration testers as well as end users understand Android security fundamentals.

What this book covers

Chapter 1, Setting Up the Lab, is an essential part of this book. This chapter will guide you to setting up a lab with all the tools that are required to follow the rest of the chapters in the book. This chapter is an essential part of the book for those who are new to Android security. It will help you build an arsenal of tools required for Android security at one place.

Chapter 2, Android Rooting, provides an introduction to the techniques typically used to root Android devices. This chapter discusses the basics of rooting and its pros and cons. Then, we shall move into topics such as the Android partition layout, boot loaders, and boot loader unlocking techniques. This chapter acts a guide for those who want to root their devices and want know the ins and outs of rooting concepts.

Chapter 3, Fundamental Building Blocks of Android Apps provides an overview of Android app internals. It is essential to understand how apps are being built under the hood, what they look like when installed on a device, how they are run, and so on. This is exactly what this chapter covers.

Chapter 4, Overview of Attacking Android Apps, provides an overview of the attack surface of Android. It discusses possible attacks on Android apps, devices, and other components in the application architecture. Essentially, this chapter lets you build a simple threat model for a traditional application that communicates with databases over the network. It is essential to understand what the possible threats that an application may come across are in order to understand what to test during a penetration test. This chapter is a high-level overview and contains fewer technical details.

Chapter 5, Data Storage and Its Security, provides an introduction to the techniques typically used to assess the data storage security of Android applications. Data storage is one of the most important elements of Android app development. This chapter begins with discussing different techniques used by developers to store data locally and how they can affect security. Then, we shall look into the security implications of the data storage choices made by developers.

Chapter 6, Server-Side Attacks, provides an overview of the attack surface of Android apps from the server side. This chapter will discuss the attacks possible on Android app backends. This chapter is a high-level overview and contains fewer technical details, as most server-side vulnerabilities are related to web attacks, which have been covered extensively in the OWASP testing and developer guides.

Chapter 7, Client-Side Attacks – Static Analysis Techniques, covers various client-side attacks from a static application security testing (SAST) viewpoint. Static analysis is a common technique of identifying vulnerabilities in Android apps caused due to the ease availability of reversing tools for Android. This chapter also discusses some automated tools available for static analysis of Android applications.

Chapter 8, Client Side Attacks – Dynamic Analysis Techniques, covers some common tools and techniques to assess and exploit client-side vulnerabilities in Android applications using dynamic application security testing (DAST). This chapter will also discuss tools such as Xposed and Frida that are used to manipulate application flow during runtime.

Chapter 9, Android Malware, provides an introduction to the fundamental techniques typically used in creating and analyzing Android malware. The chapter begins with introducing the characteristics of traditional Android malware. This chapter also discusses how to develop a simple piece of malware that gives an attacker a reverse shell on the infected phone. Finally, the chapter discusses Android malware analysis techniques.

Chapter 10, Attacks on Android Devices This chapter is an attempt to help users secure themselves from attackers while performing everyday operations, such as connecting their smartphones to free Wi-Fi access points at coffee shops and airports. This chapter also discusses why it is dangerous to root Android devices and install unknown applications.

What you need for this book

In order to get hands-on experience while reading this book, you need the following software. Download links and installation steps are shown later in the book.

- Android Studio
- An Android emulator
- Burpsuite
- Apktool
- Dex2jar
- JD-GUI
- Drozer
- GoatDroid App
- QARK
- Cydia Substrate
- Introspy
- Xposed Framework
- Frida

Who this book is for

This book is for anyone who wants to learn about Android security. Software developers, QA professionals, and beginner- to intermediate-level security professionals will find this book helpful. Basic knowledge of Android programming would be a plus.

Conventions

In this book, you will find a number of text styles that distinguish between different kinds of information. Here are some examples of these styles and an explanation of their meaning.

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "Let us first delete the `test.txt` file from the current directory."

A block of code is set as follows:

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

When we wish to draw your attention to a particular part of a code block, the relevant lines or items are set in bold:

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

Any command-line input or output is written as follows:

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

New terms and **important words** are shown in bold. Words that you see on the screen, for example, in menus or dialog boxes, appear in the text like this: "Finally, give your AVD a name and click **Finish**."

Warnings or important notes appear in a box like this.

Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or disliked. Reader feedback is important for us as it helps us develop titles that you will really get the most out of.

To send us general feedback, simply e-mail `feedback@packtpub.com`, and mention the book's title in the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide at `www.packtpub.com/authors`.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Downloading the example code

You can download the example code files for this book from your account at `http://www.packtpub.com`. If you purchased this book elsewhere, you can visit `http://www.packtpub.com/support` and register to have the files e-mailed directly to you.

You can download the code files by following these steps:

1. Log in or register to our website using your e-mail address and password.
2. Hover the mouse pointer on the **SUPPORT** tab at the top.
3. Click on **Code Downloads & Errata**.
4. Enter the name of the book in the **Search** box.
5. Select the book for which you're looking to download the code files.
6. Choose from the drop-down menu where you purchased this book from.
7. Click on **Code Download**.

You can also download the code files by clicking on the **Code Files** button on the book's webpage at the Packt Publishing website. This page can be accessed by entering the book's name in the **Search** box. Please note that you need to be logged in to your Packt account.

Once the file is downloaded, please make sure that you unzip or extract the folder using the latest version of:

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

The code bundle for the book is also hosted on GitHub at `https://github.com/PacktPublishing/hacking-android`. We also have other code bundles from our rich catalog of books and videos available at `https://github.com/PacktPublishing/`. Check them out!

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you could report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting `http://www.packtpub.com/submit-errata`, selecting your book, clicking on the **Errata Submission Form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded to our website or added to any list of existing errata under the Errata section of that title.

To view the previously submitted errata, go to `https://www.packtpub.com/books/content/support` and enter the name of the book in the search field. The required information will appear under the **Errata** section.

Piracy

Piracy of copyrighted material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works in any form on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors and our ability to bring you valuable content.

Questions

If you have a problem with any aspect of this book, you can contact us at `questions@packtpub.com`, and we will do our best to address the problem.

Table of Contents