iOS Penetration Testing

A Definitive Guide to iOS Security

—

First Edition

—

Kunal Relan

Apress®

iOS Penetration Testing

A Definitive Guide to iOS Security

First Edition

Kunal Relan

Apress®

iOS Penetration Testing: A Definitive Guide to iOS Security

Kunal Relan
Noida, Uttar Pradesh
India

ISBN-13 (pbk): 978-1-4842-2354-3 ISBN-13 (electronic): 978-1-4842-2355-0
DOI 10.1007/978-1-4842-2355-0

Library of Congress Control Number: 2016960329

Managing Director: Welmoed Spahr
Lead Editor: Nikhil Karkal
Technical Reviewer: Nishant Das Patnaik
Editorial Board: Steve Anglin, Pramila Balan, Laura Berendson, Aaron Black, Louise Corrigan, Jonathan Gennick, Robert Hutchinson, Celestin Suresh John, Nikhil Karkal, James Markham, Susan McDermott, Matthew Moodie, Natalie Pao, Gwenan Spearing
Coordinating Editor: Prachi Mehta
Copy Editor: Kezia Endsley
Compositor: SPi Global
Indexer: SPi Global
Artist: SPi Global

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a Delaware corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at www.apress.com/bulk-sales.

Any source code or other supplementary materials referenced by the author in this text are available to readers at www.apress.com. For detailed information about how to locate your book's source code, go to www.apress.com/source-code/. Readers can also access source code at SpringerLink in the Supplementary Material section for each chapter.

Printed on acid-free paper

This book is dedicated to my mom, my spiritual guru for inspiring me to live, my mentor who always supported me in this journey, and to all the weirdoes like me; I love you all.

Contents at a Glance

Contents

About the Author

Kunal Relan is an iOS security researcher and a full-stack developer who has been working as security lead for Mozilla, Delhi.

He has published several research papers on information security in the esteemed *Journal of ACM*. Having obtained the acclaimed CCNA Security certification, he is also an Owasp ZAP evangelist. With his thriving experience as a security researcher and penetration tester, Kunal is known for actively reporting security bugs in a mobile and web applications. During the past few years, he has been working as a mobile application penetration tester and a security researcher in New Delhi. Currently working as a security consultant, he is the guy behind owlpro, a WordPress security scanning platform.

About the Technical Reviewer

Nishant Das Patnaik is an experienced application security and SecDevOps engineer. He is based out of India and is currently working for eBay in Bangalore. In the past, he has worked as an AppSec and SecDevOps engineer at InMobi and Yahoo. He loves to share his work with the community as open source projects and hence has been a presenter at Black Hat Europe 2016, Black Hat USA 2016, Black Hat USA 2013, and Nullcon 2012. He loves to code on Python and JavaScript. You can reach out to him on Twitter at `@dpnishant` and check out some of his open source projects at `github.com/dpnishant`. When he is not working, you can find him playing a piano or experimenting at the kitchen.

Acknowledgments

I would personally like to thank Apress for giving me the opportunity to write this book. This book would not have been possible without the support of Nikhil Karkal, Prachi Mehta, and Suresh John. You guys have really helped a lot during the completion of this book. It has been a long journey into this amazing world of iOS development and penetration testing, the outcome of which would never have been possible without you guys. The long journey of framing the whole series into a book was possible only because of your support.

Secondly, I would like to thank my mother, who has always supported me in all the things I ever wanted to do during my journey into the field of information security. Now, years after being in information security, it's a journey I loved and spent those dark and lonely nights with, days full of passion and zeal to discover and dive deep into this area of my interest. I would also like to say thanks to Sailmn, my beloved hacker friend as he was always there as a part of motivation in my research and was one of those few who understood my vision and my passion for all of this. We spent days together working on different information security projects and he has always been so good at everything we did. Also a big thanks to all the information security books you shared with me, as they were really useful for all the things I do now. I would also like to say thanks to all my friends, family, and my mentors at Mozilla: you are the reason for me being what I am. This has been an amazing journey with you all. Lastly, a big thanks to Jay Khurana, Kunal Mohan, and all other unknown strange and weird kids we see. I have a special love for all of them; it is really hard to adjust in this world and I feel the same as you do. Keep exploring this infinite universe!

Introduction

iOS is one of the most famous mobile operating systems in the world after Android, having about 28% of total mobile operating system market. Since its release in June 2007, it has evolved, and the current stable version is iOS 9.3.3. Apple has a stronghold of the mobile market, making it the second most used mobile OS in the world. iOS is a closed source operating system, unlike its rival Android, which is open source. That makes Android the de facto mobile OS for all other hardware manufacturers including Samsung, LG, HTC, etc. Since its release in 2007, iOS has been prone to jailbreaking; however, Apple has worked hard to make the security of iOS tighter with every release. They still have not managed to avoid jailbreaking totally and the current stable version iOS 9.3.3 already has a public jailbreak available by the Pangu team, which also claims to have jailbroken the latest iOS 10 beta. This leaves a big question mark on Apple about jailbreaking and other security issues being addressed.

iOS has always been a target of attackers, with many security breaches and causalities in the past, even though Apple has been very strict with its security policies and the App Store environment, which has a lot of restrictions on app development and deployment. Apple has also been very restrictive on giving up user data APIs to developers, and has denied a lot of Private APIs for use in apps, unlike Android, which gives its users data API like SMS, call history, etc. On the top of that, it has a sandboxed application environment in the OS that isolates the application from the operating system. Even with iOS's tight architecture, app developers still manage to make their applications vulnerable to attackers, due to penetration testing and reverse engineering in iOS. This is very different from the Web or Android setup, with Android running applications built in Java, which makes it easier to reverse engineer. This book will be your guide to working with iOS penetration testing and reverse engineering, and I recommend you go through each chapter thoroughly, follow the tutorials, and try replicating them on your end.

CHAPTER 1

Introduction to iOS

iOS has been around since 2007, when we first saw the iPhone, a beautiful device with iOS in it. Developed by the Apple Macintosh team, it was originally called iPhone OS, was renamed to iOS in 2010, and now runs Apple's iPhone, iPad, and iPod Touch. It is the second most popular mobile phone in the world after Android. iOS has been around for nine years and we have seen a lot of changes since its launch. It has always been in the spotlight for its security bugs, with the first bug hitting the web in 2007.

In this chapter, we talk about how iOS works, how it manages to keep away the malware from the App Store, and how the architecture of iOS is laid out. This chapter is an introduction to iOS and covers all the basics needed to understand the coming chapters. If you already understand the architecture of iOS and its file system, you can skip this chapter and move on to the second one, but it is always a good idea to brush up on your knowledge.

Note We will be following Apple's latest 9.x and 8.x iOS versions; however, most of the features and issues are backward compatible and may work in upcoming versions as well.

iOS Introduction

iOS has been a popular operating system since its inception and its App Store has more than 1.5 million apps, of which 100 billion copies have been downloaded. iOS has always been praised for its user interface and is based on the concept of direct manipulation using multi-touch gestures. iOS shares Core Foundation and Foundation Kit frameworks with the popular OS X (the operating system in the MacBook); however, it has its own upgraded version of UIKit called Cocoa Touch. iOS also shares the Darwin foundation with OS X, which is an open source UNIX operating system released by Apple in 2000. However, iOS still doesn't provide UNIX-like shell access to users. At the time of writing this book, iOS 9.3.1 is the latest release and 9.x and 8.x are the most commonly installed releases in current devices.

Electronic supplementary material The online version of this chapter (doi: 10.1007/978-1-4842-2355-0_1) contains supplementary material, which is available to authorized users.

K. Relan, *iOS Penetration Testing*, DOI 10.1007/978-1-4842-2355-0_1