

CONTENTS IN DETAIL

FOREWORD by Alex Stamos	xix
--------------------------------	------------

ACKNOWLEDGMENTS	xxi
------------------------	------------

INTRODUCTION	xxiii
---------------------	--------------

Who This Book Is For	xxiv
What's in This Book	xxiv
How This Book Is Structured	xxiv
Conventions This Book Follows	xxvi
A Note on Swift	xxvi
Mobile Security Promises and Threats	xxvii
What Mobile Apps Shouldn't Be Able to Do	xxvii
Classifying Mobile Security Threats in This Book	xxviii
Some Notes for iOS Security Testers	xxx

PART I IOS FUNDAMENTALS

1 THE IOS SECURITY MODEL	3
-------------------------------------	----------

Secure Boot	4
Limiting Access with the App Sandbox	4
Data Protection and Full-Disk Encryption	5
The Encryption Key Hierarchy	6
The Keychain API	7
The Data Protection API	7
Native Code Exploit Mitigations: ASLR, XN, and Friends	8
Jailbreak Detection	9
How Effective Is App Store Review?	10
Bridging from WebKit	11
Dynamic Patching	11
Intentionally Vulnerable Code	12
Embedded Interpreters	12
Closing Thoughts	12

2 OBJECTIVE-C FOR THE LAZY 13

Key iOS Programming Terminology	14
Passing Messages	14
Dissecting an Objective-C Program	15
Declaring an Interface	15
Inside an Implementation File	16
Specifying Callbacks with Blocks	18
How Objective-C Manages Memory	18
Automatic Reference Counting	19
Delegates and Protocols	20
Should Messages	20
Will Messages	20
Did Messages	20
Declaring and Conforming to Protocols	21
The Dangers of Categories	22
Method Swizzling	23
Closing Thoughts	25

3 IOS APPLICATION ANATOMY 27

Dealing with plist Files	29
Device Directories	32
The Bundle Directory	33
The Data Directory	34
The Documents and Inbox Directories	34
The Library Directory	35
The tmp Directory	37
The Shared Directory	37
Closing Thoughts	38

PART II SECURITY TESTING

4 BUILDING YOUR TEST PLATFORM 41

Taking Off the Training Wheels	41
Suggested Testing Devices	42
Testing with a Device vs. Using a Simulator	43
Network and Proxy Setup	43
Bypassing TLS Validation	44
Bypassing SSL with stunnel	46

Certificate Management on a Device	47
Proxy Setup on a Device	48
Xcode and Build Setup	50
Make Life Difficult	51
Enabling Full ASLR	53
Clang and Static Analysis	54
Address Sanitizer and Dynamic Analysis	55
Monitoring Programs with Instruments	55
Activating Instruments	55
Watching Filesystem Activity with Watchdog	58
Closing Thoughts	59

5

DEBUGGING WITH LLDB AND FRIENDS

61

Useful Features in lldb	62
Working with Breakpoints	62
Navigating Frames and Variables	64
Visually Inspecting Objects	68
Manipulating Variables and Properties	69
Breakpoint Actions	70
Using lldb for Security Analysis	72
Fault Injection	72
Tracing Data	74
Examining Core Frameworks	74
Closing Thoughts	75

6

BLACK-BOX TESTING

77

Installing Third-Party Apps	78
Using a .app Directory	78
Using a .ipa Package File	80
Decrypting Binaries	80
Launching the debugserver on the Device	81
Locating the Encrypted Segment	84
Dumping Application Memory	87
Reverse Engineering from Decrypted Binaries	89
Inspecting Binaries with otool	90
Obtaining Class Information with class-dump	92
Extracting Data from Running Programs with Cycrypt	93
Disassembly with Hopper	94
Defeating Certificate Pinning	96
Hooking with Cydia Substrate	97
Automating Hooking with Introspy	100
Closing Thoughts	103

PART III SECURITY QUIRKS OF THE COCOA API

7 IOS NETWORKING 107

Using the iOS URL Loading System	108
Using Transport Layer Security Correctly	108
Basic Authentication with NSURLConnection	110
Implementing TLS Mutual Authentication with NSURLConnection	112
Modifying Redirect Behavior	113
TLS Certificate Pinning	114
Using NSURLSession	117
NSURLSession Configuration	117
Performing NSURLSession Tasks	118
Spotting NSURLSession TLS Bypasses	119
Basic Authentication with NSURLSession	119
Managing Stored URL Credentials	121
Risks of Third-Party Networking APIs	122
Bad and Good Uses of AFNetworking	122
Unsafe Uses of ASIHTTPRequest	124
Multipeer Connectivity	125
Lower-Level Networking with NSSStream	127
Even Lower-level Networking with CFStream	128
Closing Thoughts	129

8 INTERPROCESS COMMUNICATION 131

URL Schemes and the openURL Method	132
Defining URL Schemes	132
Sending and Receiving URL/IPC Requests	133
Validating URLs and Authenticating the Sender	134
URL Scheme Hijacking	136
Universal Links	137
Sharing Data with UIActivity	139
Application Extensions	140
Checking Whether an App Implements Extensions	141
Restricting and Validating Shareable Data	142
Preventing Apps from Interacting with Extensions	143
A Failed IPC Hack: The Pasteboard	144
Closing Thoughts	145

9
IOS-TARGETED WEB APPS **147**

Using (and Abusing) UIWebViews	147
Working with UIWebViews	148
Executing JavaScript in UIWebViews	149
Rewards and Risks of JavaScript-Cocoa Bridges	150
Interfacing Apps with JavaScriptCore	150
Executing JavaScript with Cordova	154
Enter WKWebView	158
Working with WKWebViews	158
Security Benefits of WKWebViews	159
Closing Thoughts	160

10
DATA LEAKAGE **161**

The Truth About NSLog and the Apple System Log	161
Disabling NSLog in Release Builds	163
Logging with Breakpoint Actions Instead	164
How Sensitive Data Leaks Through Pasteboards	164
Restriction-Free System Pasteboards	165
The Risks of Custom-Named Pasteboards	165
Pasteboard Data Protection Strategies	167
Finding and Plugging HTTP Cache Leaks	169
Cache Management	170
Solutions for Removing Cached Data	171
Data Leakage from HTTP Local Storage and Databases	174
Keylogging and the Autocorrection Database	175
Misusing User Preferences	178
Dealing with Sensitive Data in Snapshots	178
Screen Sanitization Strategies	179
Why Do Those Screen Sanitization Strategies Work?	182
Common Sanitization Mistakes	183
Avoiding Snapshots by Preventing Suspension	183
Leaks Due to State Preservation	184
Secure State Preservation	185
Getting Off iCloud to Avoid Leaks	187
Closing Thoughts	188

11
LEGACY ISSUES AND BAGGAGE FROM C **189**

Format Strings	190
Preventing Classic C Format String Attacks	191
Preventing Objective-C Format String Attacks	192

Buffer Overflows and the Stack	193
A strcpy Buffer Overflow	194
Preventing Buffer Overflows	195
Integer Overflows and the Heap	196
A malloc Integer Overflow	197
Preventing Integer Overflows	198
Closing Thoughts	198

12 INJECTION ATTACKS 199

Client-Side Cross-Site Scripting	199
Input Sanitization	200
Output Encoding	201
SQL Injection	203
Predicate Injection	204
XML Injection	205
Injection Through XML External Entities	205
Issues with Alternative XML Libraries	207
Closing Thoughts	207

PART IV KEEPING DATA SAFE

13 ENCRYPTION AND AUTHENTICATION 211

Using the Keychain	211
The Keychain in User Backups	212
Keychain Protection Attributes	212
Basic Keychain Usage	214
Keychain Wrappers	217
Shared Keychains	218
iCloud Synchronization	219
The Data Protection API	219
Protection Levels	220
The DataProtectionClass Entitlement	223
Checking for Protected Data Availability	224
Encryption with CommonCrypto	225
Broken Algorithms to Avoid	226
Broken Initialization Vectors	226
Broken Entropy	227
Poor Quality Keys	227
Performing Hashing Operations	228
Ensuring Message Authenticity with HMACs	229
Wrapping CommonCrypto with RNCrypto	230

Local Authentication: Using the TouchID	231
How Safe Are Fingerprints?	232
Closing Thoughts	232

14
MOBILE PRIVACY CONCERNS **233**

Dangers of Unique Device Identifiers	233
Solutions from Apple	234
Rules for Working with Unique Identifiers	235
Mobile Safari and the Do Not Track Header	236
Cookie Acceptance Policy	237
Monitoring Location and Movement	238
How Geolocation Works	238
The Risks of Storing Location Data	238
Restricting Location Accuracy	239
Requesting Location Data	240
Managing Health and Motion Information	240
Reading and Writing Data from HealthKit	241
The M7 Motion Processor	242
Requesting Permission to Collect Data	243
Proximity Tracking with iBeacons	244
Monitoring for iBeacons	244
Turning an iOS Device into an iBeacon	246
iBeacon Considerations	247
Establishing Privacy Policies	247
Closing Thoughts	248

INDEX **249**