

ANDROID SECURITY INTERNALS

**An In-Depth Guide to
Android's Security
Architecture**

by Nikolay Elenkov



**no starch
press**

San Francisco

ANDROID SECURITY INTERNALS. Copyright © 2015 by Nikolay Elenkov.

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

Printed in USA

First printing

18 17 16 15 14 1 2 3 4 5 6 7 8 9

ISBN-10: 1-59327-581-1

ISBN-13: 978-1-59327-581-5



Publisher: William Pollock

Production Editor: Alison Law

Cover Illustration: Garry Booth

Interior Design: Octopod Studios

Developmental Editor: William Pollock

Technical Reviewer: Kenny Root

Copyeditor: Gillian McGarvey

Compositor: Susan Glinert Stevens

Proofreader: James Fraleigh

Indexer: BIM Proofreading & Indexing Services

For information on distribution, translations, or bulk sales, please contact No Starch Press, Inc. directly:

No Starch Press, Inc.

245 8th Street, San Francisco, CA 94103

phone: 415.863.9900; info@nostarch.com

www.nostarch.com

Library of Congress Control Number: 2014952666

No Starch Press and the No Starch Press logo are registered trademarks of No Starch Press, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, we are using the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The Android robot is reproduced or modified from work created and shared by Google and used according to terms described in the Creative Commons 3.0 Attribution License.

The information in this book is distributed on an “As Is” basis, without warranty. While every precaution has been taken in the preparation of this work, neither the author nor No Starch Press, Inc. shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in it.

About the Author

Nikolay Elenkov has been working on enterprise security projects for the past 10 years. He has developed security software on various platforms, ranging from smart cards and HSMs to Windows and Linux servers. He became interested in Android shortly after the initial public release and has been developing applications for it since version 1.5. Nikolay's interest in Android internals intensified after the release of Android 4.0 (Ice Cream Sandwich), and for the past three years he's been documenting his findings and writing about Android security on his blog, <http://nelenkov.blogspot.com/>.

About the Technical Reviewer

Kenny Root has been a core contributor to the Android platform at Google since 2009, where his focus has been primarily on security and cryptography. He is the author of ConnectBot, the first SSH app for Android, and is an avid open source contributor. When he's not hacking on software, he's spending time with his wife and two boys. He is an alumnus of Stanford University, Columbia University, Chinese University of Hong Kong, and Baker College, but he's originally from Kansas City, which has the best barbecue.

BRIEF CONTENTS

Foreword by Jon Sawyer.	xvii
Acknowledgments	xix
Introduction	xxi
Chapter 1: Android's Security Model	1
Chapter 2: Permissions	21
Chapter 3: Package Management	51
Chapter 4: User Management	87
Chapter 5: Cryptographic Providers	115
Chapter 6: Network Security and PKI	145
Chapter 7: Credential Storage.	171
Chapter 8: Online Account Management	191
Chapter 9: Enterprise Security	215
Chapter 10: Device Security	251
Chapter 11: NFC and Secure Elements.	289
Chapter 12: SELinux.	319
Chapter 13: System Updates and Root Access.	349
Index	377

CONTENTS IN DETAIL

FOREWORD by Jon Sawyer	xvii
-------------------------------	-------------

ACKNOWLEDGMENTS	xix
------------------------	------------

INTRODUCTION	xxi
---------------------	------------

Who This Book Is For	xxii
Prerequisites	xxiii
Android Versions	xxiii
How Is This Book Organized?	xxiv
Conventions	xxv

1	
ANDROID'S SECURITY MODEL	1

Android's Architecture	1
Linux Kernel	2
Native Userspace	2
Dalvik VM	3
Java Runtime Libraries	4
System Services	4
Inter-Process Communication	4
Binder	5
Android Framework Libraries	10
Applications	10
Android's Security Model	12
Application Sandboxing	12
Permissions	14
IPC	15
Code Signing and Platform Keys	16
Multi-User Support	16
SELinux	17
System Updates	17
Verified Boot	18
Summary	19

2	
PERMISSIONS	21

The Nature of Permissions	21
Requesting Permissions	23
Permission Management	23
Permission Protection Levels	24
Permission Assignment	26

Permission Enforcement	30
Kernel-Level Enforcement	30
Native Daemon-Level Enforcement	31
Framework-Level Enforcement	33
System Permissions	37
Signature Permissions	39
Development Permissions	39
Shared User ID	40
Custom Permissions	42
Public and Private Components	43
Activity and Service Permissions	44
Broadcast Permissions	45
Content Provider Permissions	46
Static Provider Permissions	46
Dynamic Provider Permissions	47
Pending Intents	49
Summary	50

3

PACKAGE MANAGEMENT

51

Android Application Package Format	51
Code Signing	53
Java Code Signing	53
Android Code Signing	59
APK Install Process	61
Location of Application Packages and Data	62
Active Components	63
Installing a Local Package	66
Updating a Package	72
Installing Encrypted APKs	76
Forward Locking	79
Android 4.1 Forward Locking Implementation	80
Encrypted Apps and Google Play	82
Package Verification	83
Android Support for Package Verification	84
Google Play Implementation	85
Summary	86

4

USER MANAGEMENT

87

Multi-User Support Overview	87
Types of Users	90
The Primary User (Owner)	90
Secondary Users	91
Restricted Profiles	92
Guest User	94

User Management	95
Command-Line Tools	95
User States and Related Broadcasts	95
User Metadata	96
The User List File	96
User Metadata Files	97
User System Directory	99
Per-User Application Management	99
Application Data Directories	100
Application Sharing	101
External Storage	104
External Storage Implementations	104
Multi-User External Storage	105
External Storage Permissions	111
Other Multi-User Features	112
Summary	113

5 CRYPTOGRAPHIC PROVIDERS 115

JCA Provider Architecture	116
Cryptographic Service Providers	116
JCA Engine Classes	119
Obtaining an Engine Class Instance	119
Algorithm Names	120
SecureRandom	120
MessageDigest	121
Signature	122
Cipher	123
Mac	127
Key	128
SecretKey and PBEKey	128
PublicKey, PrivateKey, and KeyPair	129
KeySpec	129
KeyFactory	129
SecretKeyFactory	130
KeyPairGenerator	131
KeyGenerator	131
KeyAgreement	132
KeyStore	133
CertificateFactory and CertPath	135
CertPathValidator and CertPathBuilder	136
Android JCA Providers	137
Harmony's Crypto Provider	137
Android's Bouncy Castle Provider	137
AndroidOpenSSL Provider	140
OpenSSL	142
Using a Custom Provider	142
Spongy Castle	143
Summary	144

6 NETWORK SECURITY AND PKI 145

PKI and SSL Overview	146
Public Key Certificates	146
Direct Trust and Private CAs	148
Public Key Infrastructure	148
Certificate Revocation	150
JSSE Introduction	151
Secure Sockets	152
Peer Authentication	152
Hostname Verification	154
Android JSSE Implementation	155
Certificate Management and Validation	156
Certificate Blacklisting	162
Reexamining the PKI Trust Model	166
Summary	170

7 CREDENTIAL STORAGE 171

VPN and Wi-Fi EAP Credentials	172
Authentication Keys and Certificates	172
The System Credential Store	173
Credential Storage Implementation	174
The keystore Service	174
Key Blob Versions and Types	176
Access Restrictions	176
keymaster Module and keystore Service Implementation	176
Nexus 4 Hardware-Backed Implementation	178
Framework Integration	180
Public APIs	181
The KeyChain API	181
KeyChain API Implementation	185
Controlling Access to the Keystore	186
Android Keystore Provider	188
Summary	189

8 ONLINE ACCOUNT MANAGEMENT 191

Android Account Management Overview	192
Account Management Implementation	192
AccountManagerService and AccountManager	193
Authenticator Modules	194
The Authenticator Module Cache	194
AccountManagerService Operations and Permissions	195
The Accounts Database	198
Multi-User Support	201
Adding an Authenticator Module	203

Google Accounts Support	206
The Google Login Service	206
Google Services Authentication and Authorization	209
Google Play Services	211
Summary	213

9 ENTERPRISE SECURITY 215

Device Administration	216
Implementation	217
Adding a Device Administrator	223
Enterprise Account Integration	226
VPN Support	229
PPTP	229
L2TP/IPSec	229
IPSec Xauth	230
SSL-Based VPNs	230
Legacy VPN	231
Application-Based VPNs	236
Multi-User Support	239
Wi-Fi EAP	242
EAP Authentication Methods	243
Android Wi-Fi Architecture	244
EAP Credentials Management	245
Adding an EAP Network with WifiManager	248
Summary	250

10 DEVICE SECURITY 251

Controlling OS Boot-Up and Installation	252
Bootloader	252
Recovery	253
Verified Boot	254
dm-verity Overview	254
Android Implementation	255
Enabling Verified Boot	256
Disk Encryption	258
Cipher Mode	259
Key Derivation	260
Disk Encryption Password	261
Changing the Disk Encryption Password	262
Enabling Encryption	263
Bootting an Encrypted Device	265
Screen Security	268
Lockscreen Implementation	268
Keyguard Unlock Methods	269
Brute-Force Attack Protection	276

Secure USB Debugging	277
ADB Overview	277
The Need for Secure ADB	279
Securing ADB	280
Secure ADB Implementation	281
ADB Authentication Keys	282
Verifying the Host Key Fingerprint	282
Android Backup	283
Android Backup Overview	283
Backup File Format	284
Backup Encryption	286
Controlling Backup Scope	287
Summary	288

11 NFC AND SECURE ELEMENTS 289

NFC Overview	289
Android NFC Support	290
Reader/Writer Mode	290
Peer-to-Peer Mode	294
Card Emulation Mode	295
Secure Elements	295
SE Form Factors in Mobile Devices	296
Accessing the Embedded SE	299
Android SE Execution Environment	302
UICC as a Secure Element	305
Software Card Emulation	310
Android 4.4 HCE Architecture	310
APDU Routing	311
Writing an HCE Service	315
Security of HCE Applications	317
Summary	318

12 SELINUX 319

SELinux Introduction	320
SELinux Architecture	320
Mandatory Access Control	321
SELinux Modes	322
Security Contexts	322
Security Context Assignment and Persistence	324
Security Policy	324
Policy Statements	324
Type Transition Rules	327
Domain Transition Rules	328
Access Vector Rules	329
Android Implementation	330
Kernel Changes	331
Userspace Changes	332
Device Policy Files	339
Policy Event Logging	340

Android 4.4 SELinux Policy	340
Policy Overview	341
Enforcing Domains	342
Unconfined Domains	344
App Domains	345
Summary	347

13

SYSTEM UPDATES AND ROOT ACCESS 349

Bootloader	350
Unlocking the Bootloader	350
Fastboot Mode	352
Recovery	354
Stock Recovery	354
Custom Recoveries	363
Root Access	364
Root Access on Engineering Builds	365
Root Access on Production Builds	368
Rooting by Changing the boot or system Image	369
Rooting by Flashing an OTA Package	370
Rooting via Exploits	375
Summary	376

INDEX 377