



Exam Code: AND - 402

# Android Version 5 Security Essentials

Android Security Essentials



- Understand Android's security model and architecture.
- Build Android applications with security best practices in mind.
- Build more robust applications that appeal to clients.
- Build a new Android application for each Android security lesson.

By Android ATC Team

[www.androidatc.com](http://www.androidatc.com)

Android ATC

# Android™ Security Essentials

Course Code: AND-402 version 5

Hands on Guide to Android Security Principles

# Android™ Security Essentials

## Course Code: AND-402 version 5

Copyrights © 2015 Android ATC

Published by: Android ATC

First Printing May 2015.

ISBN: 978-0-9900143-5-5

Information in this book, including URL and other Internet Web site references, is subject to change without notice. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Android ATC.

Android ATC is not responsible for webcasting or any other form of transmission received from any linked site. Android ATC is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Android ATC of the site or the products contained therein.

Android ATC may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except when expressly provided in any written license agreement from Android ATC, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Android Security Essentials is a detailed guide on the basics of Android security best practices. The book is accompanied with practical hands on examples, illustrations, and practical labs. It will help you build your Android application with security in mind.

Lessons in this book cover a wide range of security related topics. It starts off with a through guide on Android permissions then moves to the manipulation of application policy. It also explains the principles of user privacy followed a guide on all secure data storage techniques available in Android system.

### Warning and Disclaimer

This book is designed to provide information about “Android Security Essentials” course with exam AND-402. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

### Exam

You may test your knowledge of the content in this book by taking the online AND-402 exam through Pearson VUE worldwide testing centers. Passing this exam is a leading step towards the path of becoming an “Android Certified Application Engineer”. For more information, visit: <http://www.pearsonvue.com/androidatc>

## Trade Mark Acknowledge

All terms mentioned in this book are known to be trademarks or service marks that have been appropriately capitalized. Use of a term in this book should not be regarded as affecting the validity of any trade mark or service mark.

Android is a trademark of Google Inc. 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.

## About This Course

This is a two-day (12 hours) professional course, which thoroughly covers the Android™ security model and concerns of both the developer and end-user point of view.

## Course Prerequisite

It's highly recommended that the attendees of this course know the basics of Android application development knowledge. To acquire good knowledge of Android application development, trainees may attend the "Android Application Development" course provided by Android ATC

## Upon completing this course, students will be able to:

- 1- Understand Android software architecture.
- 2- Understand Android's security model.
- 3- Build Android applications with security best practices in mind.
- 4- Build more secure and more robust application that appeals to clients.

# Table of Contents

## Lesson 1 Permissions

<b>Introduction</b> .....	1-2
<b>Android Platform Architecture</b> .....	1-2
<b>Android Security Architecture</b> .....	1-3
Application signing.....	1-3
Installing applications.....	1-4
<b>Permissions</b> .....	1-4
Why Permissions.....	1-4
Enforcing permissions.....	1-5
<b>Levels of Protection</b> .....	1-5
Normal Permissions or Level-Zero Permissions.....	1-5
Dangerous Permissions or Level-one Permissions.....	1-6
Signature Permission or Level-two Permissions.....	1-7
Signature and System Permissions or Level-three Permissions.....	1-8
<b>Application Level Permissions</b> .....	1-9
Adding system permissions required by an application.....	1-9
Declaring permissions required by other applications.....	1-11
<b>Component level Permissions</b> .....	1-12
Activity.....	1-13
Service.....	1-14
Content Providers.....	1-15
Broadcast Intents.....	1-15
<b>Extending Android Permissions</b> .....	1-16
Adding a new permission.....	1-17
Creating a permission group.....	1-18
Creating a permission tree.....	1-19
	1-20
<b>Lab 1: Securing Applications Using Permission</b> .....	
Create an application to use Permission.....	1-21
Create permission and access it.....	1-32

## Lesson 2 Managing the Policy File

<b>Introduction</b> .....	2-2
<b>The Manifest File</b> .....	2-2
Attributes of Manifest Tag.....	2-4
Attributes of Application Tag.....	2-5
<b>Modifying Application Policy</b> .....	2-8
Applications running with the same Linux ID.....	2-8
Setting application permissions.....	2-9
Permissions for external applications.....	2-9
External storage.....	2-10
Debugging Mode.....	2-11
Backup.....	2-12
	2-13
<b>Lab 2: Defining the Application's Policy File</b> .....	
Creating two applications with the same Linux ID.....	2-14
Backing up Data on Cloud Storage.....	2-26
Debugging the Application.....	2-37
Moving application to the Internal Memory of the Device.....	2-41

## Lesson 3 User Data Privacy and Protection

<b>Introduction</b> .....	3-2
<b>Data security principles</b> .....	3-2
Confidentiality.....	3-2
Integrity.....	3-2
Availability.....	3-2
The mobile environment.....	3-3
Data states.....	3-4
<b>Vulnerabilities and Attacks against Stored Data</b> .....	3-4
Vulnerabilities of Stored Data.....	3-4
Threats to Stored Data.....	3-5
<b>Protection Principles</b> .....	3-5
<b>Digital rights management</b> .....	3-6
Tips for Android Coding Vulnerabilities.....	3-8
	3-9
<b>Lab 3: Data Confidentiality and Protection</b> .....	
Lab 3-1: Ensuring Data Confidentiality.....	3-10
Lab 3-2 : Protecting Application Data with Permissions.....	3-28

## Lesson 4 Securing Storage

<b>Introduction</b> .....	4-2
<b>Data storage decisions</b> .....	4-2
Privacy.....	4-2
Data storage period.....	4-2
<b>Storage Mechanisms</b> .....	4-2
<b>Shared preferences</b> .....	4-3
Creating a preference file.....	4-3
Writing preference.....	4-4
Preference Activity.....	4-5
<b>File</b> .....	4-5
Creating a file.....	4-5
Writing to a file.....	4-6
Reading from a file.....	4-6
File operations on an external storage.....	4-7
<b>Cache</b> .....	4-8
Reading preference.....	4-4
<b>Database</b> .....	4-9
	4-12
<b>Lab 4: Data Storage Applications</b> .....	
Using Shared Preferences.....	4-13
File Storage Operations.....	4-19
Storing data in Cache.....	4-45
SQLite Database Storage.....	4-53
Retrieve Gmail Account Info Using Account Manager.....	4-61