1.

Record Nr.	UNINA9910453383103321
Autore	Makan Keith
Titolo	Android security cookbook / / Keith Makan, Scott Alexander-Brown
Pubbl/distr/stampa	Birmingham : , : Packt Publishing, , 2013
ISBN	1-78216-717-X
Edizione	[1st edition]
Descrizione fisica	1 online resource (350 p.)
Altri autori (Persone)	Alexander-BrownScott
Disciplina	005.258
Soggetti	Operating systems (Computers) - Security measures Smartphones - Security measures Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover; Copyright; Credits; About the Authors; About the Reviewers; www.PacktPub.com; Table of Contents; Preface; Chapter 1: Android Development Tools; Introduction; Installing the Android Development Tools (ADT); Installing the Java Development Kit (JDK); Updating the API sources; Alternative installation of the ADT; Installing the Native Development Kit (NDK); Emulating Android; Creating Android Virtual Devices (AVDs); Using the Android Debug Bridge (ADB) to interact with the AVDs; Copying files off/onto an AVD; Installing applications onto the AVDs via ADB Chapter 2: Engaging with Application SecurityIntroduction; Inspecting application certificates and signatures; Signing Android applications; Verifying application signatures; Inspecting the AndroidManifest.xml file; Interacting with the activity manager via ADB; Extracting application resources via ADB; Chapter 3: Android Security Assessment Tools; Introduction; Installing and setting up Santoku; Setting up drozer; Running a drozer session; Enumerating installed packages; Enumerating activities; Enumerating content providers; Enumerating services; Enumerating broadcast receivers Determining application attack surfacesLaunching activities; Writing a drozer module - a device enumeration module; Writing an application certificate enumerator; Chapter 4: Exploiting Applications; Introduction; Information disclosure via logcat; Inspecting network traffic; Passive intent sniffing via the activity manager; Attacking services; Attacking

broadcast receivers; Enumerating vulnerable content providers; Extracting data from vulnerable content providers; Inserting data into content providers; Enumerating SQL-injection vulnerable content providers; Exploiting debuggable applications
Man in the middle attacks on applicationsChapter 5: Protecting Applications; Introduction; Securing application components; Protecting components with custom permissions; Protecting content provider paths; Defending against SQL injection attack; Application signature verification (anti-tamper); Tamper protection by detecting the installer, emulator, and debug flag; Removing all log messages with ProGuard; Advanced code obfuscation with DexGuard; Chapter 6: Reverse Engineering Applications; Introduction; Compiling from Java to DEX; Decompiling DEX files; Interpreting the Dalvik bytecode
Decompiling DEX to JavaDecompiling application native libraries; Debugging the Android processes using the GDB server; Chapter 7: Secure Networking; Introduction; Validating self-signed SSL certificates; Using StrongTrustManager from the OnionKit library; SSL pinning; Chapter 8: Native Exploitation and Analysis; Introduction; Inspecting file permissions; Cross-compiling native executables; Exploitation of race condition vulnerabilities; Stack memory corruption exploitation; Automated native Android fuzzing; Chapter 9: Encryption and Developing Device Administration Policies; Introduction
Using cryptography libraries

Sommario/riassunto

Android Security Cookbook' breaks down and enumerates the processes used to exploit and remediate Android app security vulnerabilities in the form of detailed recipes and walkthroughs."" Android Security Cookbook"" is aimed at anyone who is curious about Android app security and wants to be able to take the necessary practical measures to protect themselves; this means that Android application developers, security researchers and analysts, penetration testers, and generally any CIO, CTO, or IT managers facing the impeding onslaught of mobile devices in the business environment will benefit from