Inspeckage

Android Package Inspector

Antonio Martins, Hack In The Box 2016
antonio@tempest.com.br

What is it about?

- Tool
  - Inspeckage is a tool developed to offer dynamic analysis of Android applications. By applying hooks to functions of the Android API, Inspeckage will help you understand what an Android application is doing at runtime.
- Audience
  - Developers, testers, pen-testers, security researchers, paranoids, etc

Who am I?

- Antonio Carlos Martins
  - Recife, Pernambuco, Brazil
  - github.com/ac-pm

Who am I?

- Security Consultant @ Tempest Security Intelligence
  - http://www.tempest.com.br/en/
- Member of Mobile Cell
  - A group of researchers of Tempest with focus on mobile

São Paulo - BR
Recife - BR
London - UK

Agenda

- Mobile Testing Methodology
- Blackbox Analysis
- Inspeckage
- Demo

Mobile Testing Methodology

- Information Gathering
  - What networking protocols are in use?
  - Does the application perform commerce transactions?
  - What frameworks are in use?
  - Etc.

Mobile Testing Methodology

- Information Gathering
  - What networking protocols are in use?
  - Does the application perform commerce transactions?
  - What frameworks are in use?
  - Etc.
- Static Analysis
  - Analyzing source code obtained from development team
  - If the source is not available, decompile the application's binary

Mobile Testing Methodology

- Information Gathering
  - What networking protocols are in use?
  - Does the application perform commerce transactions?
  - What frameworks are in use?
  - Etc.
- Static Analysis
  - Analyzing source code obtained from development team
  - If the source is not available, decompile the application's binary
- Dynamic Analysis
  - Monitor logged messages and notifications generated at runtime
  - Observe IPC between the target application and other applications
  - Attach a debugger using JDB to step through code execution

Blackbox Analysis

In a time-constrained we must answer:

- How the app works? (without the source code)
- How it interact with the other components?
- What are the security issues?

Blackbox Analysis

In a time-constrained we must answer:

- How the app works? (without the source code)
- How it interact with the other components?
- What are the security issues?

Inspeckage can help us!

Inspeckage - How it Works

- Simple application (apk)
- Internal HTTP server
- Friendly web interface
- Developed as an Xposed Framework Module

Inspeckage - How it Works

- Simple application (apk)
- Internal HTTP server
- Friendly web interface
- Developed as an Xposed Framework Module

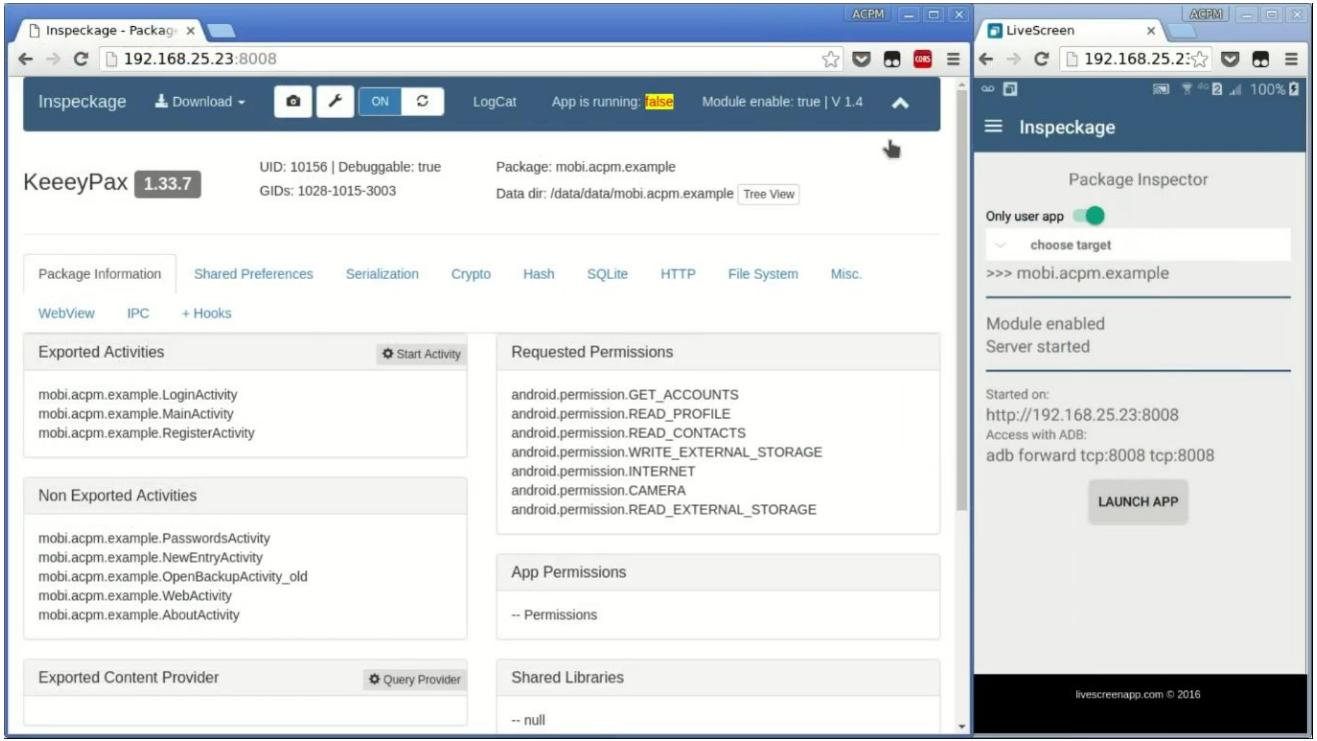
You can run it without Xposed!

https://play.google.com/store/apps/details?id=mobi.acpm.inspeckage

Inspeckage - Features

- Information gathering
- Actions (with the app)
- Android Configurations
- Extras (screenshot, downloads)
- Hooks (some APIs)
- + Hooks (add new hooks)
- Logcat (experimental)

Demo


Inspeckage - Packag
192.168.25.23:8008
Inspeckage
Download
ON
LogCat
App is running: false
Module enable: true | V 1.4
KeeeyPax 1.33.7
UID: 10156 | Debuggable: true
GIDs: 1028-1015-3003
Package: mobi.acpm.example
Data dir: /data/data/mobi.acpm.example
Tree View
Package Information
Shared Preferences
Serialization
Crypto
Hash
SQLite
HTTP
File System
Misc.
WebView
IPC
+ Hooks
Exported Activities
Start Activity
mobi.acpm.example.LoginActivity
mobi.acpm.example.MainActivity
mobi.acpm.example.RegisterActivity
Non Exported Activities
mobi.acpm.example.PasswordsActivity
mobi.acpm.example.NewEntryActivity
mobi.acpm.example.OpenBackupActivity_old
mobi.acpm.example.WebActivity
mobi.acpm.example.AboutActivity
Exported Content Provider
Query Provider
Requested Permissions
android.permission.GET_ACCOUNTS
android.permission.READ_PROFILE
android.permission.READ_CONTACTS
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.INTERNET
android.permission.CAMERA
android.permission.READ_EXTERNAL_STORAGE
App Permissions
-- Permissions
Shared Libraries
-- null
LiveScreen
Inspeckage
Package Inspector
Only user app
choose target
>>> mobi.acpm.example
Module enabled
Server started
Started on:
http://192.168.25.23:8008
Access with ADB:
adb forward tcp:8008 tcp:8008
LAUNCH APP
livescreenapp.com © 2016

Download latest 1.3

Inspeckage

- Google Play
  - https://play.google.com/store/apps/details?id=mobi.acpm.inspeckage
- Xposed Module Repository
  - http://repo.xposed.info/module/mobi.acpm.inspeckage
- Xposed Installer
  - Download App
- GitHub
  - https://github.com/ac-pm/Inspeckage

References

- ADB - http://developer.android.com/intl/pt-br/tools/help/adb.html
- Acpm.mobi – https://acpm.mobi/genymotion-xposed-inspeckage/
- Android Developer - http://developer.android.com/intl/pt-br/develop/index.html
- AndroidXRef - http://androidxref.com/
- Dashboards - http://developer.android.com/intl/pt-br/about/dashboards/index.html
- Genymotion - https://www.genymotion.com
- Inspeckage - https://github.com/ac-pm/Inspeckage
- LiveScreen - https://play.google.com/store/apps/details?id=com.livescreenapp.free
- Remote Debugging - https://developer.chrome.com/devtools/docs/remote-debugging
- TeamWin - TWRP - https://twrp.me/
- Xposed - https://github.com/rovo89/Xposed
- Xposed for Lollipop and Marshmallow - http://forum.xda-developers.com/showthread.php?t=3034811
- Xposed Module Repository - http://repo.xposed.info/module/mobi.acpm.inspeckage

Thank you!

Antonio Martins, Hack In The Box 2016
antonio@tempest.com.br