

How to attack an Android app

Knowledge Friday

Benjamin Adolphi <benjamin@promon.no>

whoami

- Head of the security research at Promon.
- Breaking and securing apps since 2011.
- Passionate reverse engineer.
- Love to break things.

Introduction

- Teaching you how to attack simple Android apps.
- Foundation for solving challenge.
- Material: <https://github.com/badolphi/knowledge-friday>

Reverse engineering

- Understanding how an app works.
- Reveal secrets in it.
- First step of an attacker.
- Two complementary approaches: Static and dynamic
- On Android
 - Java code (Java, Kotlin)
 - Native code (C, C++, Dart, ...)

Reverse engineering Java code

- Code in classes.dex file(s).
- Dalvik bytecode executed in VM.
- Requires disassembler¹ or decompiler².



¹ <https://github.com/iBotPeaches/Apktool>

² <https://github.com/skylot/jadx>

Reverse engineering native code

- Code is found in .so files.
- Executed directly on the CPU.
- There are many good disassemblers/decompilers ^{1,2,3,4}.



¹ <https://hex-rays.com/ida-pro>

² <https://binary.ninja>

³ <https://github.com/NationalSecurityAgency/ghidra>

⁴ <https://rada.re>

Demo

Repackaging

- Modifying app on disk.
- Change code to change behavior.
- Change resources to change look.

Patching Java code

- Modify classes.dex file(s).
- Direct binary patching can be tricky.
- Tools like apktool make this easy
 - Disassemble to smali.
 - Modify smali.
 - Re-assemble to apk.
 - Sign.



Patching Native code

- Modify .so file(s).
- Can be done manually.
- Disassemblers/decompilers usually make this easier.
- Requires available space.

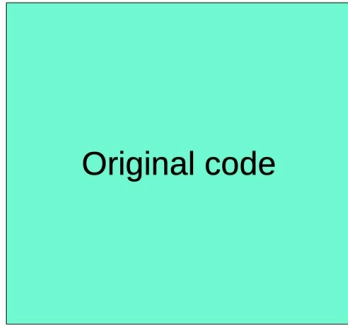
Demo

Hooking

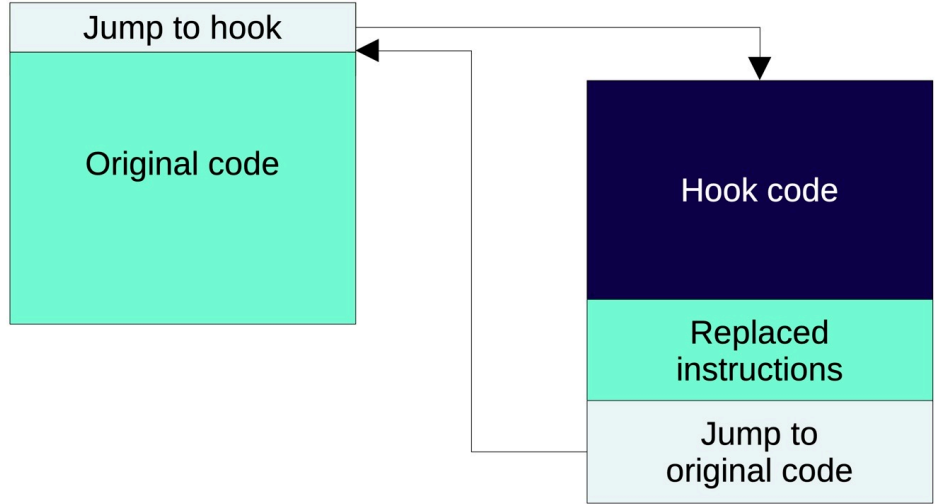
- Modify the app while it runs.
- Change code to change behavior.
- Useful for dynamic reverse engineering.

How hooking works

Before



After



PROMON

Hooking Java code

- Code is executed in VM.
- Could be compiled ahead of time or just in time.
- Requires modifying the VM.
- Popular hooking frameworks
 - LSPosed¹
 - Frida²



FRIDA

¹ <https://github.com/LSPosed/LSPosed>

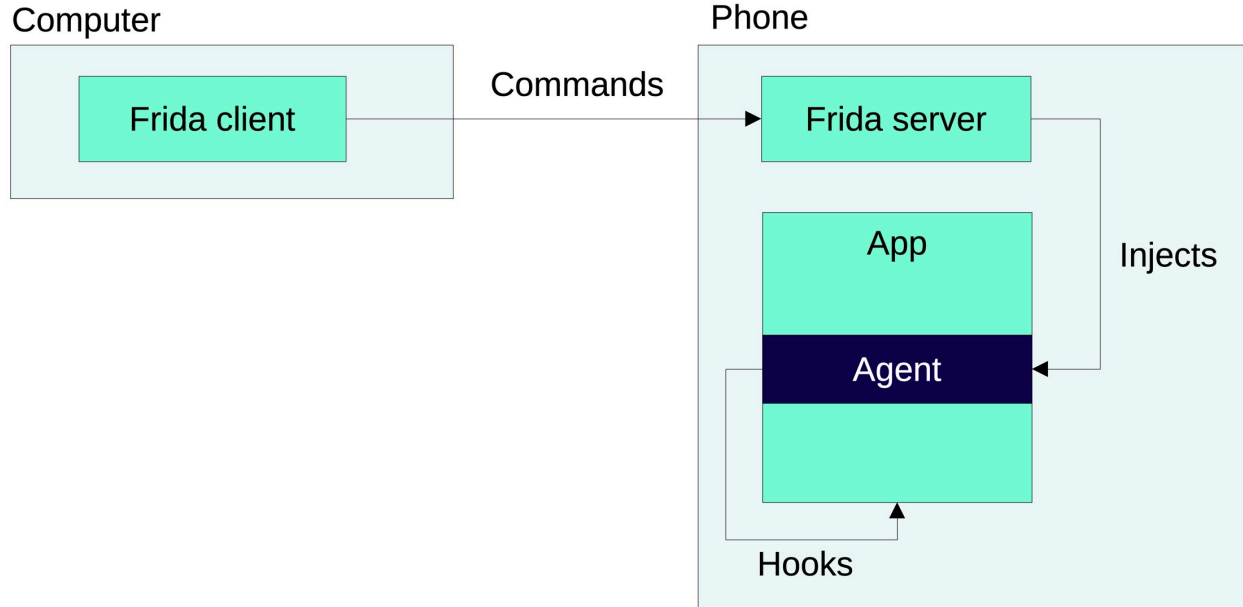
² <https://frida.re>

Hooking native code

- Overwrite code in memory.
- Not completely trivial.
- Frida is a popular framework to use.

FRIDA

How Frida works in our use case



Demo

Challenge

- Two apps that you should attack.
- Using one of the presented attacks.
- A successful attack will give you a flag.

Thank you!



Benjamin Adolphi
Head of Security Research
benjamin@promon.no