PROMON

Game On - The Art of Hacking an Android App

NSConnect24

Benjamin Adolphi <benjamin@promon.de>

# whoami

- Head of the security research at Promon.
- Breaking and securing apps since 2011.
- Passionate reverse engineer.
- Huge Frida fan.

Introduction

- Thinking like an attacker helps you in protecting your apps.
- Teaching you how to attack simple Android apps.
- Material: https://github.com/badolphi/nsconnect24

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 disassembler[1] or decompiler[2].

[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

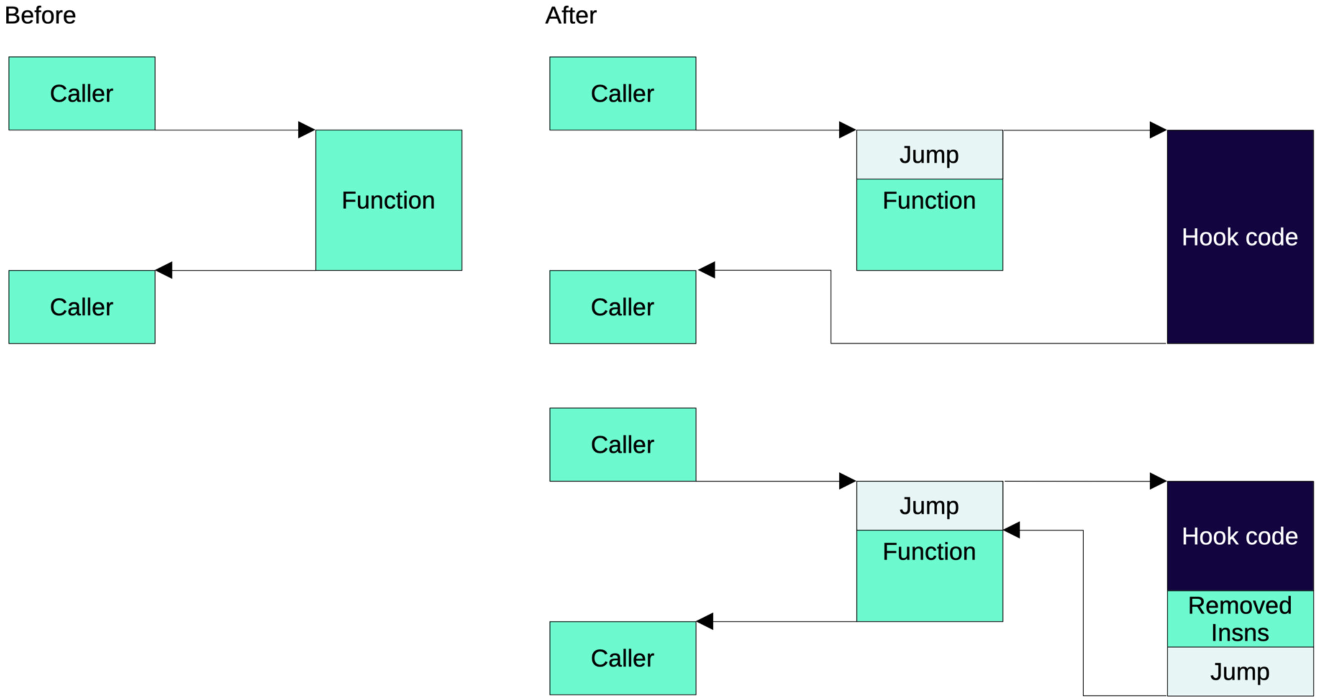
- Modify .so file(s).
- Can be done manually.
- Disassemblers/decompilers usually make this easier.
- Requires available space.

Demo

Hooking

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

How hooking works



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
  - LSPosed[1]
  - Frida[2]

[1] https://github.com/LSPosed/LSPosed

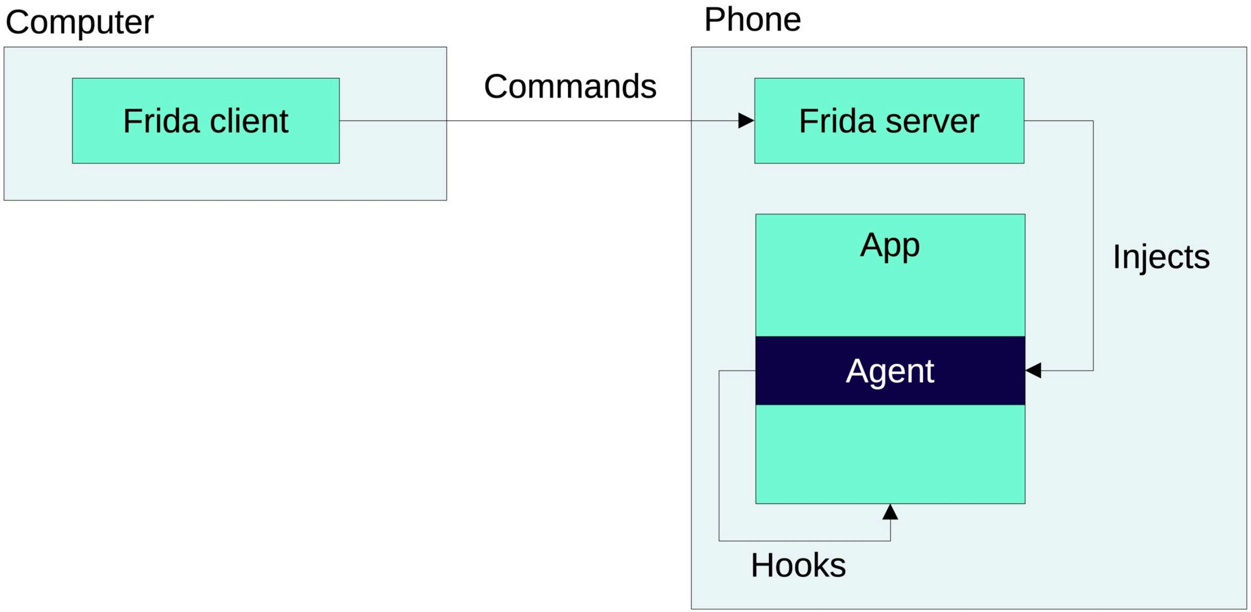
[2] https://frida.re

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



PROMON

Demo

PROMON

Thank you!

Benjamin Adolphi
Head of Security Research
benjamin@promon.de