Mobile Security - Android Instrumentation using Frida

by Lukas Treffner & Hans-Jürgen Kleeberger

Frida - Overview

FRIDA
DYNAMIC INSTRUMENTATION TOOLKIT

- Open-source dynamic instrumentation framework for Android, iOS, Linux Windows, and macOS
- Allows analyzing and manipulating application behavior by providing an easy-to-learn scripting interface
- Scripts can be injected during application runtime
- Relies on a client-server architecture by injecting the “frida-server” into the target process being the server and using “frida-tools” as the client.

Frida – Usecases

FRIDA
DYNAMIC INSTRUMENTATION TOOLKIT

- for tracing method invocations of target applications
- for modifying and observing application behavior
  - by modifying or logging argument/return values of instrumented methods

Frida – CLI

- frida-ps
  - Lists all processes
- frida-discover
  - Lists all function calls in an app
- frida-ls-devices
  - Lists attached devices
- frida-kill
  - Kills a process

Frida CLI – “frida-trace”

FRIDA
DYNAMIC INSTRUMENTATION TOOLKIT

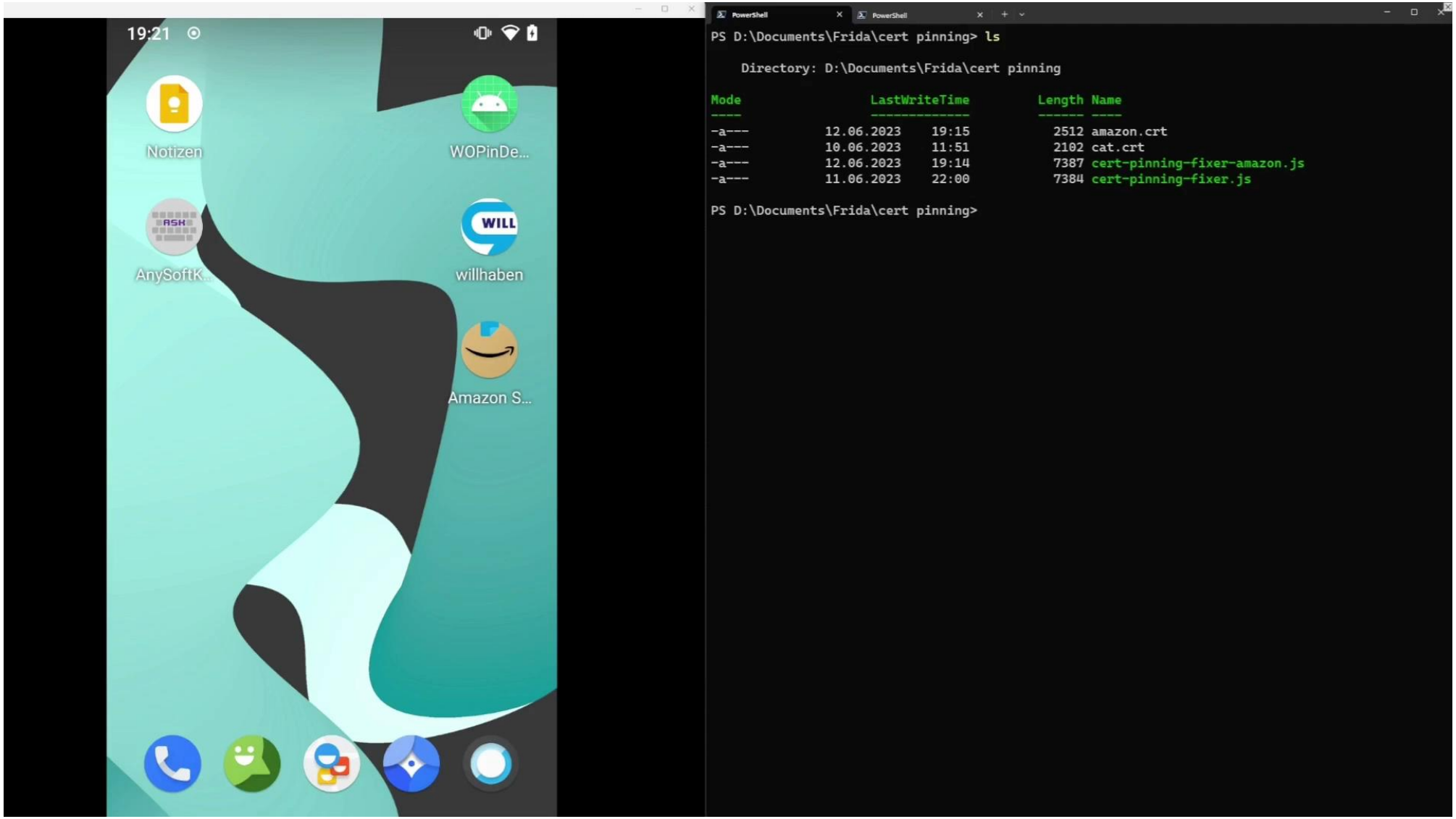
- allows to instrument processes without the need of writing dedicated scripts

```
PS D:\Documents\Frida> frida-trace -U -f at.willhaben -j '*!*certificate*/isu'
Instrumenting...
HMSPackageManager.isUseOldCertificate: Auto-generated handler at "D:\\Documents\\Frida\\__handlers__\\com.huawei.hms.utils.HMSPackageManager\\isUseOldCertificate.js"
HMSPackageManager.setUseOldCertificate: Auto-generated handler at "D:\\Documents\\Frida\\__handlers__\\com.huawei.hms.utils.HMSPackageManager\\setUseOldCertificate.j
s"
a.$init: Auto-generated handler at "D:\\Documents\\Frida\\__handlers__\\okhttp3.a\\_init.js"
RealConnection$connectTls$1.$init: Auto-generated handler at "D:\\Documents\\Frida\\__handlers__\\okhttp3.internal.connection.RealConnection_connectTls_1\\_init.js"
d.a: Auto-generated handler at "D:\\Documents\\Frida\\__handlers__\\sr.d\\a.js"
d.c: Auto-generated handler at "D:\\Documents\\Frida\\__handlers__\\sr.d\\c.js"
Started tracing 6 functions. Press Ctrl+C to stop.
           /* TID 0x4e51 */
  1308 ms  HMSPackageManager.isUseOldCertificate()
  1309 ms  <= false
           /* TID 0x4ebf */
  1356 ms  a.$init("config.mpianalytics.com", 443, "<instance: okhttp3.m, $className: com.google.android.gms.internal.measurement.v5>", "<instance: javax.net.SocketF
actory, $className: javax.net.DefaultSocketFactory>", "<instance: javax.net.ssl.SSLSocketFactory, $className: com.android.org.conscrypt.OpenSSLSocketFactoryImpl>", "
<instance: javax.net.ssl.HostnameVerifier, $className: sr.d>", "<instance: okhttp3.CertificatePinner>", "<instance: okhttp3.b, $className: v.o>", null, "<instance: j
ava.util.List, $className: java.util.Collections$UnmodifiableRandomAccessList>", "<instance: java.util.List, $className: java.util.Collections$UnmodifiableRandomAcce
ssList>", "<instance: java.net.ProxySelector, $className: sun.net.spi.DefaultProxySelector>")
  1502 ms  d.c("<instance: java.security.cert.X509Certificate, $className: com.android.org.conscrypt.OpenSSLX509Certificate>", "config.mpianalytics.com")
  1506 ms  <= true
```

Certificate Pinning Fixer

- Adding pinning an already built android application
- Use of network security config pinning
- No need to rebuilt/know/have source code
- No interference with original implementation

Demo

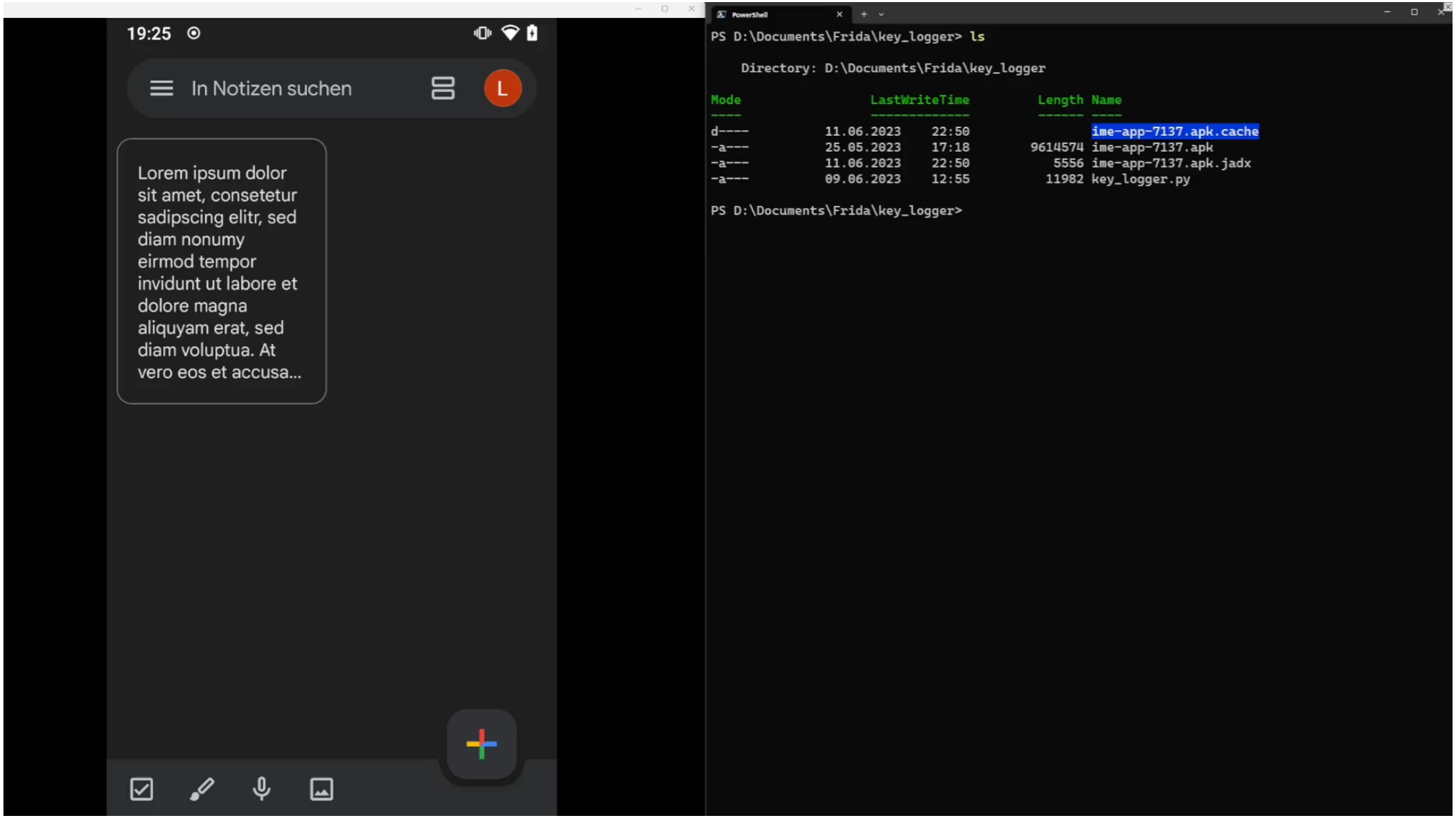

19:21
Notizen
WOPinDe...
AnySoftK...
willhaben
Amazon S...
PowerShell
PowerShell
PS D:\Documents\Frida\cert pinning> ls
Directory: D:\Documents\Frida\cert pinning
Mode LastWriteTime Length Name
-a--- 12.06.2023 19:15 2512 amazon.crt
-a--- 10.06.2023 11:51 2102 cat.crt
-a--- 12.06.2023 19:14 7387 cert-pinning-fixer-amazon.js
-a--- 11.06.2023 22:00 7384 cert-pinning-fixer.js
PS D:\Documents\Frida\cert pinning>

Keylogger

FRIDA
DYNAMIC INSTRUMENTATION TOOLKIT

- Focus on AnySoft Keyboard
- Simple logging of user input
- Outputting user input in python script

Demo


19:25
In Notizen suchen
L
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusa...
PowerShell
PS D:\Documents\Frida\key_logger> ls
Directory: D:\Documents\Frida\key_logger
Mode LastWriteTime Length Name
d---- 11.06.2023 22:50 ime-app-7137.apk.cache
-a--- 25.05.2023 17:18 9614574 ime-app-7137.apk
-a--- 11.06.2023 22:50 5556 ime-app-7137.apk.jadx
-a--- 09.06.2023 12:55 11982 key_logger.py
PS D:\Documents\Frida\key_logger>