Reversing
Flutter
Applications
with Radare2
And Frida

- Govind Sharma, Thales
- R2con 2024

#### Who am I?



**Govind Sharma** 

# Mobile Security Engineer at Thales, @apkunpacker

Specializing in pentesting Android and iOS applications, I focus on identifying vulnerabilities, performing code audits, and conducting comprehensive security assessments

# What tools we need?

Radare2 - apt install radare2

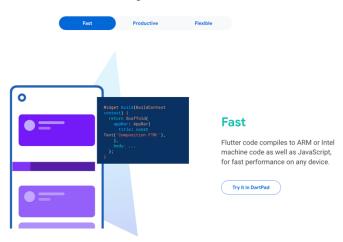
Frida – pip install Frida Frida-tools

### Agenda



### Flutter in Brief - https://flutter.dev

Flutter is an open source framework for building beautiful, natively compiled, multi-platform applications from a single codebase.



# **Dart** is an **object**-oriented programming language with a **C-style** syntax

```
class Hello {
  void sayHello() {
    print("Welcome to
    R2Con2024");
void main() {
  var hello = Hello();
  hello.sayHello();
```

# Asynchronous functions and Futures

```
Future < String > doPost(String arg) async {
    var response = await http.post(
        Uri.parse('http://127.0.0.1:9000'),
        body: { 'a' : arg }
    );
    return response.body;
}
```

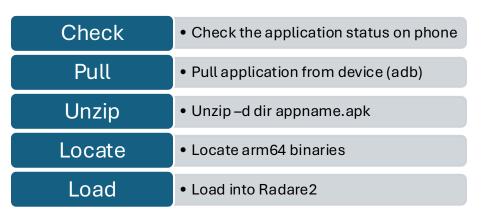
- Keyword async
- Keyword await means to wait for the future to complete
- A future is the result of an async operation.

# Late initialization

late is used to indicate a variable is initializer later

```
late final String _data;
@override
void initState() {
   super.initState();
   // Initialize _data here
   _data = "Initialized data";
}
```

# Back to Reversing:



#### Radare2 cheatsheet

#### r2 [-i scripts] binary

- f entry: List all flags (labels) which contain the word entry
- s 0x1234: Seek/Go to address 0x1234
- pdf: Disassemble a function
- pd 10: Disassemble 10 instructions at current address
- axt @ 0x1234:
   Showxref functions of 0x1234

- aa: Analyze All
- af: Defines a function at the current location
- afl: List all functions
- ie: Show entry point
- is: Show symbols
- .script.r2.js: Execute plugininscript.r2.js file
- /x 010000d4: Search for bytes

### Flutter Apps

libflutter.so is an ELF shared library. There's an ELF header, sections, etc.

Unlike libapp.so, it does not contain AOT snapshots or Dart VM payloads.

libflutter.so provides the Flutter engine, which includes Skia for rendering, text layout, plugins, platform channels, and the runtime environment for executing Dart code.

```
Disassembly
                                                                         | = Functions
                                                                                                                 [& cache]
         0x001c5708
                         .strina "FieldInitializer" : len=17
                                                                           0x009c3860
                                                                                                16 sym.imp.pthread_self
         ;-- str.DartVMInitializer:
                                                                           0x009c3870
                                                                                                16 sym.imp.abort
           STRN XREFS from fcn.0080d7c8 @ 0x80dd80(w), 0x80eec4(w)
                                                                           0x009c3880
                                                                                                16 sym.imp.strlen
         0x001c570b
                         .string "DartVMInitializer"; len=18
                                                                           0x009c3890
                                                                                                16 sym.imp.eglCreateWindow
         ;-- str.Canvas::saveLayer:
                                                                           0x009c38a0
                                                                                                16 sym.imp.eqlCreatePbuffe
                                    STRN 0x004cc498 STRN 0x004cd68c
STRN 0x006dcb7c STRN 0x0073f028
                                                                          0x009c38b0
                                                                                                16 sym.imp.ealGetCurrentCo
                                                                        51 0x009c38c0
                                                                                                16 sym.imp.eglMakeCurrent
         0x001c571d
                         .string "Canvas::saveLayer"; len=18
                                                                           0x009c38d0
                                                                                                16 sym.imp.eqlChooseConfid
         :-- str.EngineLaver:
                                                                           0x009c38e0
                                                                                                16 sym.imp.ealCreateConte
         0x001c572f
                         .string "EngineLayer"; len=12
                                                                           0x009c38f0
                                                                                                16 sym.imp.eqlDestroyConte
         :-- str.RasterCacheFlow::Layer:
          STRN XREF from fcn.006db9a8 @ 0x6dba44(w)
                                                                          = Symbols
                                                                                                                 [& cache]
                         .string "RasterCacheFlow::Layer"; len=23
         0x001c573b
                                                                           0x00459e50 3920 JNI_OnLoad
                                                                           0x000ea680 817232 _binary_icudtl_dat_start
         :-- str.lower:
         0x001c5752
                         .string "lower" : len=6
                                                                           0x001b1ed0 0 _binary_icudtl_dat_size
         :-- str.nssslserver:
                                                                           0x009c3860 16 imp.pthread_self
                         .string "nssslserver"; len=12
         0x001c5758
                                                                           0x009c3870 16 imp.abort
         ;-- str.ssl_server:
                                                                           0x009c3880 16 imp.strlen
                                                                          0x009c3890 16 imp.eqlCreateWindowSurface
```

# R2 in Action

# App throws error if cert check fail:



Error: HandshakeException: Handshake error in client (OS Error:



CERTIFICATE\_VERIFY\_ FAILED: unable to getlocal issuer certificate(handshake. cc:393))

Keep attention on file name: line number

#### R2 in action:

```
[0x0043b4c0]> iz~+ssl
23053 0x001bc867 0x001bc867 10
                                  11
                                       .rodata ascii
                                                       ssl client
24583 0x001c5764 0x001c5764 10
                                  11
                                       .rodata ascii
                                                       ssl_server
28547 0x001db6cb 0x001db6cb 58
                                  59
                                       .rodata ascii
                                                        ../../flutter/third_party/boringssl/src/ssl/ssl_privkey.cc
28563 0x001dba18 0x001dba18 59
                                  60
                                       .rodata ascii
                                                        ../../flutter/third_party/boringssl/src/ssl/ssl_aead_ctx.cc
28574 0x001dbc7f 0x001dbc7f 55
                                  56
                                                        ../../flutter/third_party/boringssl/src/ssl/ssl_cert.cc
                                       rodata ascii
28576 0x001dbce1 0x001dbce1 61
                                  62
                                       .rodata ascii
                                                        ../../flutter/third_party/boringssl/src/ssl/ssl_transcript.cc
28599 0x001dc1ad 0x001dc1ad 59
                                  60
                                                        ../../flutter/third_party/boringssl/src/ssl/ssl_versions.cc
                                       rodata ascii
28650 0x001dccd5 0x001dccd5 57
                                  58
                                       .rodata ascii
                                                        ../../flutter/third_party/boringssl/src/ssl/ssl_cipher.cc
28656 0x001dce0e 0x001dce0e 57
                                  58
                                                        ../../flutter/third_party/boringssl/src/ssl/ssl_buffer.cc
                                       rodata ascii
28673 0x001dd158 0x001dd158 58
                                  59
                                       .rodata ascii
                                                        ../../flutter/third_party/boringssl/src/ssl/ssl_session.cc
28715 0x001dda29 0x001dda29 60
                                  61
                                       rodata ascii
                                                        ../../flutter/third_party/boringssl/src/ssl/ssl_kev_share.cc
                                                        ../../flutter/third_party/boringssl/src/ssl/ssl_lib.cc
28750 0x001de0eb 0x001de0eb 54
                                  55
                                       .rodata ascii
28758 0x001de297 0x001de297 55
                                  56
                                                        ../../flutter/third_party/boringssl/src/ssl/ssl_x509.cc
                                       .rodata ascii
28760 0x001de307 0x001de307 55
                                  56
                                                        ../../flutter/third_party/boringssl/src/ssl/ssl_asn1.cc
                                       .rodata ascii
29913 0x001e59d3 0x001e59d3 12
                                       .rodata ascii
                                                       SSL_CERT_DIR
39880 0x00270a31 0x00270a31 16
                                                       BAD SSL FILETYPE
                                       .rodata ascii
39952 0x002710ee 0x002710ee 19
                                  20
                                       .rodata ascii
                                                        INVALID_SSL_SESSION
39985 0x002713c4 0x002713c4 12
                                  13
                                       .rodata ascii
                                                       NULL SSL CTX
                                  23
39986 0x002713d1 0x002713d1 22
                                       .rodata ascii
                                                       NULL_SSL_METHOD_PASSED
40037 0x0027196e 0x0027196e 34
                                  35
                                       .rodata ascii
                                                       SSL CTX HAS NO DEFAULT SSL VERSION
40038 0x00271991 0x00271991 21
                                       rodata ascii
                                                       SSL_HANDSHAKE_FAILURE
40039 0x002719a7 0x002719a7 31
                                  32
                                       .rodata ascii
                                                       SSL_SESSION_ID_CONTEXT_TOO_LONG
                                  24
40040 0x002719c7 0x002719c7 23
                                       .rodata ascii
                                                       SSL_SESSION_ID_TOO_LONG
40087 0x00271ef6 0x00271ef6 19
                                  20
                                       .rodata ascii
                                                       UNKNOWN SSL VERSION
40101 0x00272052 0x00272052 17
                                  18
                                       .rodata ascii
                                                       WRONG_SSL_VERSION
```

### R2 in action:

Look	Look for Xref Functions
Match	Match with BoringSSL
Help	Error Code and Line Number can help

#### Frida in Action:

```
Interceptor.attach(Module.findExportByName(null, 'android_dlopen_ext'), {
    onEnter: function (args) {
        var library = args[0].readCString()
        if (library.includes('libflutter.so')) {
           this.hook = true:
    onLeave: function (retval) {
        if (this.hook) {
            var libapp = Module.findBaseAddress('libflutter.so');
            Interceptor.attach(libapp.add(0x6d1c90), {
                onleave: function (retval) {
                    console.log(`[+] session_verify_cert_chain retval: ${retval}`);
                    retval.replace(0x1);
            });
```

#### R2 in action:



Thanks for your attention!

# Special thanks to:

Pancake Cryptax AbhiTheModder