

 DWASP GLOBAL **AppSec**

ViE'26
NNA JUN
25-26

25

years
of open source security

OWASP GLOBAL AppSec

ViE'26
NNA JUN
25-26

25

years
of open source security

Unveiling The Internals Of Multiplatform Mobile App Runtimes

by **PANCAKE** (aka **SERGI ÀLVAREZ i CAPILLA**)

Who am I?

- Sergi Alvarez i Capilla (aka **pancake**)
- Author of **radare2** and other free software projects
- Mobile **Security Research** Engineer at **NowSecure**



Why radare2?

- It's my toy project ^^
- Fast, portable, flexible, extensible and opensource RE toolkit
- One toolkit support all those binaries.
 - From native to virtual machine architectures
- Commandline, GUI, Web and AI/MCP
- Integrates with Frida, Renef, Jadx, Gdb and native debugger
 - r2pm package manager for extra plugins

01

Radare2

CLI/GIT

```
$ git clone https://github.com/radareorg/radare2  
$ radare2/sys/install.sh
```

GUI/IAITO

```
https://github.com/radareorg/iaito
```

MCP

```
$ r2pm -ci r2ai r2mcp
```

The Mobile Triad

- Mobile App Development Ecosystem is WILD
- Crossplatform development frameworks are SAVAGE
- Custom VMs, Obfuscations, AOT, Crazy Optimizations, DSLs..

02

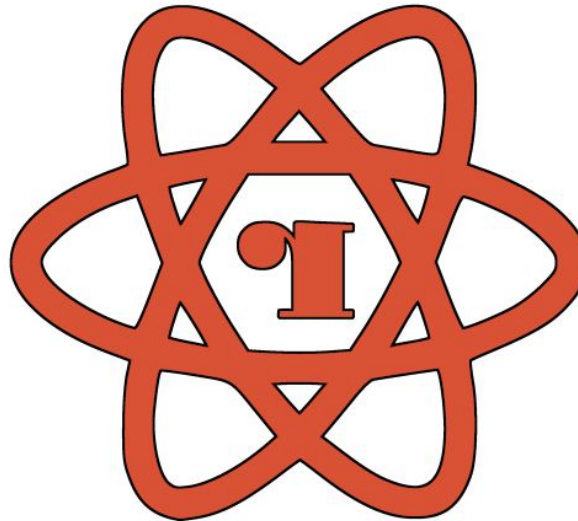
The Mobile Triad

UNITY
(CSharp)



```
r2pm -ci r2unity
```

REACT NATIVE
(JavaScript)



```
r2pm -ci r2hermes
```

FLUTTER
(Dart)



```
r2pm -ci r2flutter
```

Time Constraints

This could be a **4 day training**, but I have just **30 minutes** 🤖
..so I will focus on the most interesting low level and fun details.

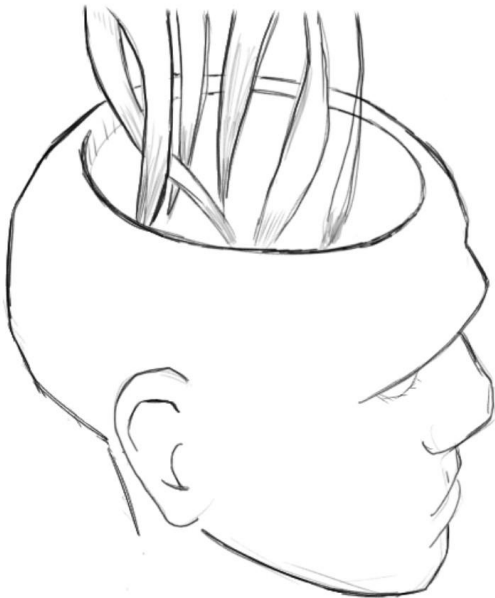
- Install r2/iaito/r2ai/r2mcp and the respective plugins
- All those plugins are written in plain C, zero dependencies
- Actively fuzzed, Audited with AI and several static analysis

Reversing Layers

Symbols, Type, Strings

Analysis, XRefs & SBOM

Emulation and Decompilation



Unity

- Transpiles C# to C++ and ECMA blob
- Android, iOS, Windows, macOS, Switch..
- Designed for videogame development

03



Unity Metadata

- It's MSIL, so it's following the ECMA335 from 2012
- **Global-metadata.dat** => function names, signatures and more
- IL2CPP Executable = code, addresses, field offsets, runtime tables
- From v24 (2017-2024) to v38 (Unity6 - 2025-2026)
 - **SBOM!!** - Components, versions and dependencies
 - ReversePInvoke resolutions may give us Native calls
 - We map metadata with il2cpp via the CodeRegistration struct array, which is accessed by ldr[]



Unity 6000 (Late 2024+)

- We need the **Il2CppCodeRegistration** symbol
 - Heuristic (stripped), Deterministic (debug), User provided
- U6K exposes per-module method arrays, before it was flat global
- Only function addresses are resolved, null pointers are interfaces



OLD

```
g_CodeRegistration
-> methodPointersCount
-> methodPointers[]
```

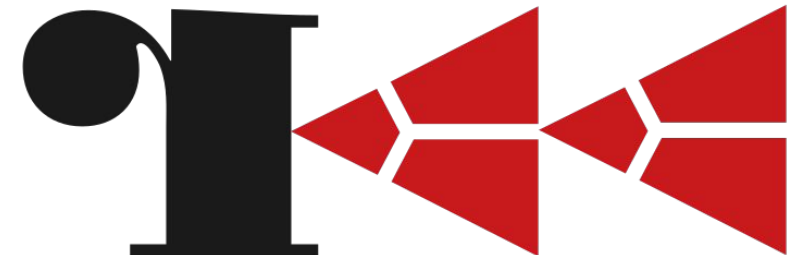
NEW

```
g_CodeRegistration
-> codeGenModulesCount
-> codeGenModules[]
    -> methodPointerCount
    -> methodPointers[]
```

Idiomatic Decompilation

- Fully annotated native code is perfect for LLMs to
- LLM assisted decompilation plugins for radare2: **r2ai** or **Decai**

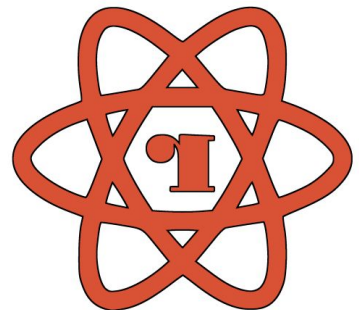
```
$ r2 -e r2ai.lang=csharp ...  
[0x00000000]> decai -e lang=csharp
```



React Native

- Also known as Hermes / HBC
- Javascript bytecode VM by **Meta**
 - 256 x 32bit registers
- Source in TypeScript
- FFI Native Components

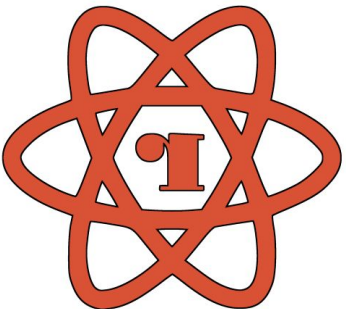
04



Buffer Literals (aka SLP)

- Since v97, Create Arrays and Objects (JSON-like) of any kinds
- All configuration files, hardcoded credentials, network headers..
 - `new_object_from_buffer` / `new_array_from_buffer` / ...

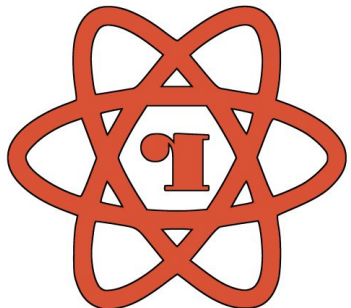
```
load_const_string r9, 0x2f6ba ; str.onScrollToTop
; 0x1002f6ba ; "onScrollToTop"
put_new_own_by_id_short r8, r9, 0x218ca ; str.registrationName
; 0x100218ca ; "registrationName"
put_new_own_by_id r6, r8, 0x2983d ; str.topScrollToTop
; 0x1002983d ; "topScrollToTop"
put_new_own_by_id_short r3, r6, 0x20740 ; str.dir
; 0x10020740 ; "dir"
try_get_by_id r9, r4, 1, 0x1ed15 ; str.Object
; 0x1001ed15 ; "Object"
get_by_id_short r8, r9, 12, 0x1fa80 ; str.assignValue
; 0x1001fa80 ; "assignValue"
new_object_with_buffer r6, 38, 38, 1533, 668 ; 0x100377a1
; lit.obj.0x377a1
{alwaysBounceHorizontal: true, alwaysBounceVertical: true,
```



Interlaced Strings

Strings are **utf16** and **non-null** terminated

- They can overlap, patching is difficult:
 - Same address + different lengths
 - Different address + overlapped in length



R2 is the only RE tool capable
with Ctypes to Codemeta

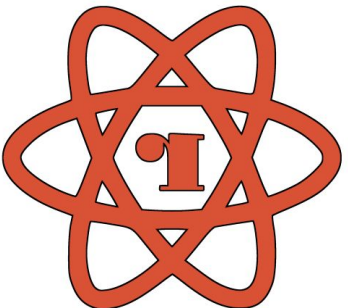
```
hermes same address
[0x0019eeda]> pd 1
    ;-- str.runAnimation:
    ;-- str.runAnimations:
    0x0019eeda      .string "runAnimations" ; len=13
[0x0019eeda]> x 16
- offset - DADB DCDD DEDF E0E1 E2E3 E4E5 E6E7 E8E9 ABCDEF0123456789
0x0019eeda 7275 6e41 6e69 6d61 7469 6f6e 732c 7570 runAnimations,up
[0x0019eeda]> []

r2hermes demo
[0x003f0611]> pd 2
    ;-- str.Subtotal:
    0x003f0611      .string "Subtotal" ; len=8
    ;-- str.totalWrap:
    0x003f0614      .string "totalWrap" ; len=9
[0x003f0611]> x 16
- offset - 1112 1314 1516 1718 191A 1B1C 1D1E 1F20 123456789ABCDEF0
0x003f0611 5375 6274 6f74 616c 5772 6170 702f 6e65 SubtotalWrapp/ne
[0x003f0611]> []
```


Evil Eval

- Inject JS code, easily obfuscatable
- V95 introduced a 3rd strict parameter
 - Ut8 treated as a boolean
 - `eval("x=1",1)` // crash if x undefined
- DirectEval opcode calls `global.eval` if previously overridden
- Use `pd:h` to decompile and understand the string evaluated, usually computed at runtime or obfuscated

```
[0x1003a2cc]> r2hermes-Ej~{  
[  
  {  
    "address": 269293163,  
    "function_id": 4953,  
    "offset": 40,  
    "function_address": 269293123,  
    "name": "onPress"  
  }  
]  
[0x1003a2cc]> pi 1 @ 269293163  
direct_eval r0, r0, 0  
[0x1003a2cc]>
```



Flutter

- Dart is like a clean TypeScript
- Developed from Google
- Mix between a VM and AOT
- Also permits FFI calls
- Different structs on iOS/Android

05



ObjectPool, PP and x27

A mix between Java's constant pool and MIPS global pointer.

- We need a custom calling convention (doc/[dyncc.md](https://github.com/OWASP/AndroidSecurity/blob/master/Documentation/dyncc.md))
- On ARM64, x4 describes arguments
 - Arity/Type/Name metadata
 - Highly Dynamic Functions (megamorphic) use the x5 register to specify the InlineCacheData, asprovides provides info about the receiver class

```
x4=ArgDescriptor  
x5=InlineCacheData  
x24=CodeObjectId  
x26=ThreadObjectId  
x27=PoolPointer
```

```
dyncc:x1,x2,x3,x5,x6,x7,^0,^1:x0!dx4!tx26!cx24!gx27!C(x26,x27,x24,x5)
```



Unstable ObjectPool ABI

- Flutter version is determined by an md5 hash of the snapshot source files of the vm
- To break static analysis tools we must patch both vm and bin hashes
- We ship a table of stable releases

- Every release and devbuild change the “constants”

Dart VM	PatchClass	Library	Namespace	Code	Object Pool	Array	String	OneByteString	NumPredefined
2.10.0	5	13	14	16	20	78	80	81	156
2.13.0	5	11	12	15	18	75	77	78	148
2.14.0	5	12	13	16	20	79	81	82	152
2.15.0	6	13	14	17	21	79	82	83	153
2.19.0	6	13	14	17	21	89	92	93	176
3.0.5	6	13	14	18	22	90	93	94	177
3.4.3	6	13	14	18	22	89	92	93	174
3.10.7	6	13	14	18	23	90	93	94	175

Dart Functions

The Snapshot Cluster contains an **InstructionTable (IT)**

- References the beginning of all the functions in the binary
- Each entry exposes type and reflection information, so it's indexed
- NativeFunctions are clearly identified, so it's easy to find FFI calls

Code is constructed optimized to lack clear function boundaries..



```
$ r2 -e anal.flagbounds=true
```

Dart Strings

- Strings can be Latin1 or UTF16 (not utf8) .. OneByteString, TwoByteString
 - Fixed size runes, length in tagged pointers or encoded in the snapshot
 - Tagged pointers can be demangled with r2flutter -O
 - Not null terminated, but usually null padded, parser stops on non-printable
- Heuristically categorized as: app, library or runtime
 - Used for SBOM when no pubspec.lock/.dart_tool/package_config.json



```
Runtime: dart: dartvm dart/  
Library: package: .dart /lib  
Applica: Other
```

Questions?

Email at pancake@nopcode.org

Fediverse [@pancake@infosec.exchange.org](https://infosec.exchange/@pancake)

06



VIENNA'26 JUN 25-26

25 years
of open source security

THANK YOU!