R2Frida

overdrivecon2019

pancake

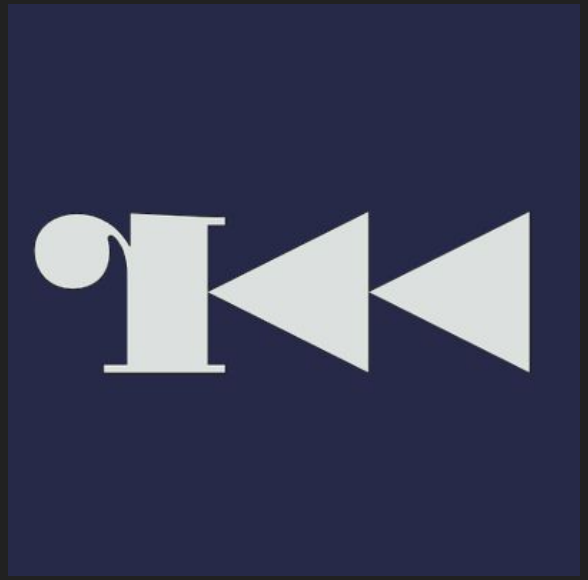
Who am I

- My name is **Sergi ÀIvarez i Capilla**
  - But most people know me as **pancake**
- Author of **radare2**, **r2frida**, **applesign**, **fsmon**, **valabind**, **acr**, **0xFFFF**, and many, many other open source tools out there.

- Senior Mobile Security Research Engineer
- Working at **NowSecure**
- Spend my time building new tools and find new ways to improve our products that make safer Mobile apps.

What's r2?

- Srsly?
  - Do i really need to explain this again?

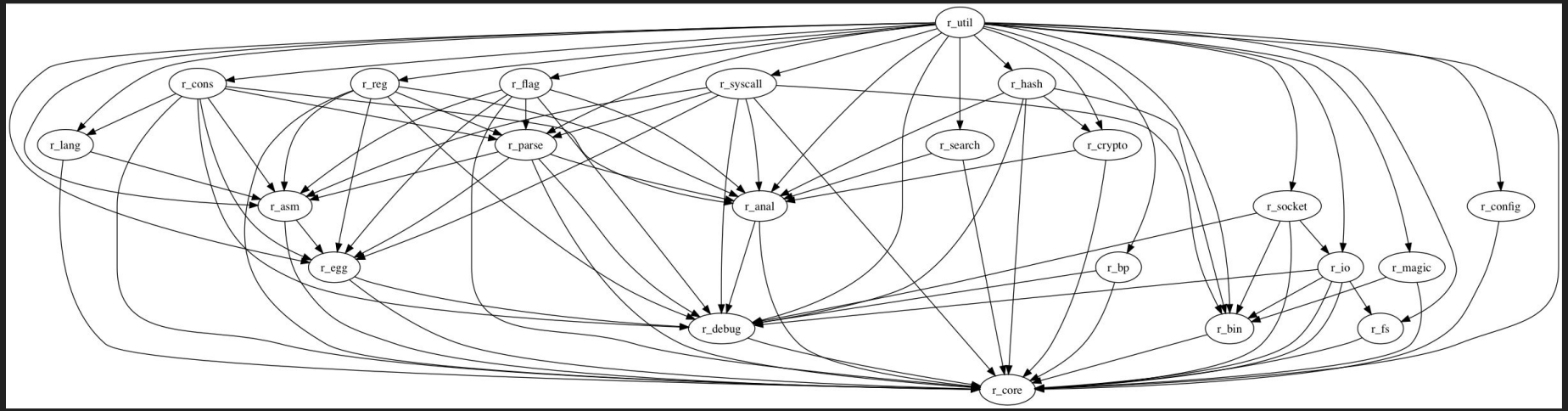


R2 Ecosystem

R2Land is the place where everyone using or makng r2 lives.

- We have humans (non-standard ones)
- Cookies and grapes
- Yearly conference
- 0 Dependencies (posix or nt)
- Plugins
- Scripts
- Modules
- R2pm

R2Land Map


r_util
r_cons
r_reg
r_flag
r_syscall
r_hash
r_lang
r_parse
r_search
r_crypto
r_asm
r_anal
r_socket
r_config
r_egg
r_bp
r_io
r_magic
r_debug
r_bin
r_fs
r_core

Recent improvements in r2

Everytime i have to do a talk i use to fix some issues that happen when i prepare the slides and demos...

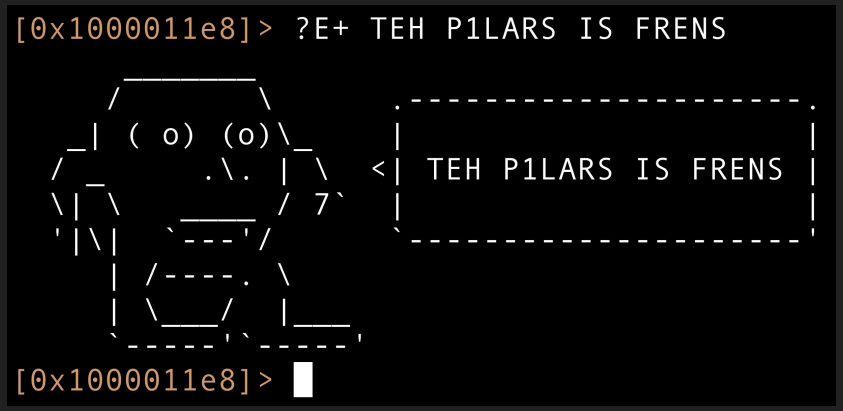
This time i have 6 talks in 1 week... so i decided not to prepare any demos for this talk at all. \o/

So here's a pic of my cat ^w^

Jk, but she lives in r2land too

No srsly, what can you do in r2land?

- Buy pizzas
- Make music and demoscene
- Know your referendum voting place
- Chat to clippy or orang AI
- Disassemble, debug and analyze funky binaries



Latest in r2?

- Main dev focus on stability and API cleanup
- Improved panels support
- Improved graph navigation
- Many new visual modes (ropchain, refs browser)
- Faster support for big binaries
- Much better disasm visualization
- Cutter users look happy

Frida

Dynamic instrumentation toolkit written by my colleague Ole André

- Written in C with bindings for JavaScript and Python
- It's the best introspection tooling for iOS and Android
- Injects an egg with a JS interpreter into the target process.
- At this point you can instrument the entire process with js
  - Provides APIs to read/write memory, list symbols, add traces, ..
  - Modify the behaviour or trace protocols, APIs, behaviours, ..

R2Frida

It's an IO Plugin for r2 that allows to connect to a Frida instance.

- Localhost, Network or USB
- Spawn or Attach

New stuff in Frida

- Crashlog retrieval for iOS/Android
- Shorter APIs and more OO
- New Kernel APIs for tfp0
- ChromeDev tools

Modifying a program in memory

```
Count 0 / 62
Count 0 / 63
Count 0 / 64
Count 0 / 65
Count 0 / 66
Count 0 / 67
Count 31337 / 68
Count 31337 / 69
Count 31337 / 70
Count 31337 / 71
Count 31337 / 72
Count 31337 / 73
Count 31337 / 74
```

```c
/* example program for r2frida demo */

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <stdbool.h>

int i = 0;
int j = 0;

int main() {
  i = 0;
  j = 0;
  while (true) {
    printf ("Count %d / %d\n", i, j);
    sleep (1);
    j++;
  }
  return 0;
}
```

```
(fcn) sym.fun.main 97
  int sym.fun.main (int argc, char **argv, char **envp);
          ; var int32_t var_ch @ rbp-0xc
          ; var int32_t var_8h @ rbp-0x8
          ; var int32_t var_4h @ rbp-0x4
          0x1059b5f10      55              push rbp
          0x1059b5f11      4889e5          mov rbp, rsp
          0x1059b5f14      4883ec10        sub rsp, 0x10
          0x1059b5f18      c745fc000000.   mov dword [var_4h], 0
          0x1059b5f1f      c705f7000000.   mov dword [sym.var.i], 0          ; sym.sec.i ; [0x1059b6020:4]=0
          0x1059b5f29      c705f1000000.   mov dword sym.var.j, 0            ; sym.sec.j ; [0x1059b6024:4]=57 ; "9"
          ; CODE XREFS from sym.fun.main (0x1059b5f10, 0x1059b5f6c)
      ┌─> 0x1059b5f33   *  8b35e7000000   mov esi, dword [sym.var.i]        ; sym.sec.i ; [0x1059b6020:4]=0
      ╎   0x1059b5f39      8b15e5000000   mov edx, dword sym.var.j          ; sym.sec.j ; [0x1059b6024:4]=57 ; "9"
      ╎   0x1059b5f3f      488d3d5e0000.  lea rdi, [0x1059b5fa4]            ; "Count %d / %d\n"
      ╎   0x1059b5f46      b000           mov al, 0
      ╎   0x1059b5f48      e825000000     call imp.printf                   ;[1] ; int printf(const char *format)
      ╎   0x1059b5f4d      bf01000000     mov edi, 1
      ╎   0x1059b5f52      8945f8         mov dword [var_8h], eax
      ╎   0x1059b5f55      e81e000000     call imp.sleep                    ;[2] ; int sleep(int s)
      ╎   0x1059b5f5a      8b15c4000000   mov edx, dword sym.var.j          ; sym.sec.j ; [0x1059b6024:4]=57 ; "9"
      ╎   0x1059b5f60      83c201         add edx, 1
      ╎   0x1059b5f63      8915bb000000   mov dword sym.var.j, edx          ; sym.sec.j ; [0x1059b6024:4]=57 ; "9"
      ╎   0x1059b5f69      8945f4         mov dword [var_ch], eax
      └─< 0x1059b5f6c      e9c2ffffff     jmp 0x1059b5f33
          0x1059b5f71      90             nop
          ;-- fcn.1059b5f72:
(fcn) imp.printf 6
  int imp.printf (const char *format);
          ; CALL XREFS from sym.fun.main (0x1059b5f10, 0x1059b5f48)
          0x1059b5f72      ff2598000000   jmp qword reloc.null.printf_1     ; [0x1059b6010:8]=0x7fff75064ec4 sym.imp.print
          ;-- fcn.1059b5f78:
(fcn) imp.sleep 6
  int imp.sleep (int s);
          ; CALL XREFS from sym.fun.main (0x1059b5f10, 0x1059b5f55)
Press <enter> to return to Visual mode.00   jmp qword reloc.null.sleep_2      ; [0x1059b6018:8]=0x7fff7509e74d sym.imp.sleep
:> wai mov esi, 31337
Written 5 byte(s) ( mov esi, 31337) = wx be697a0000
:>
```

Injecting code

- The dxc command will call a function with the arguments we provide.
- We can also write code directly...
- Memory page permissions
- Using wai or the visual assembler

Searching patterns or code

- Use the / to search in r2... use the \/ to search in r2frida

Carving the heap

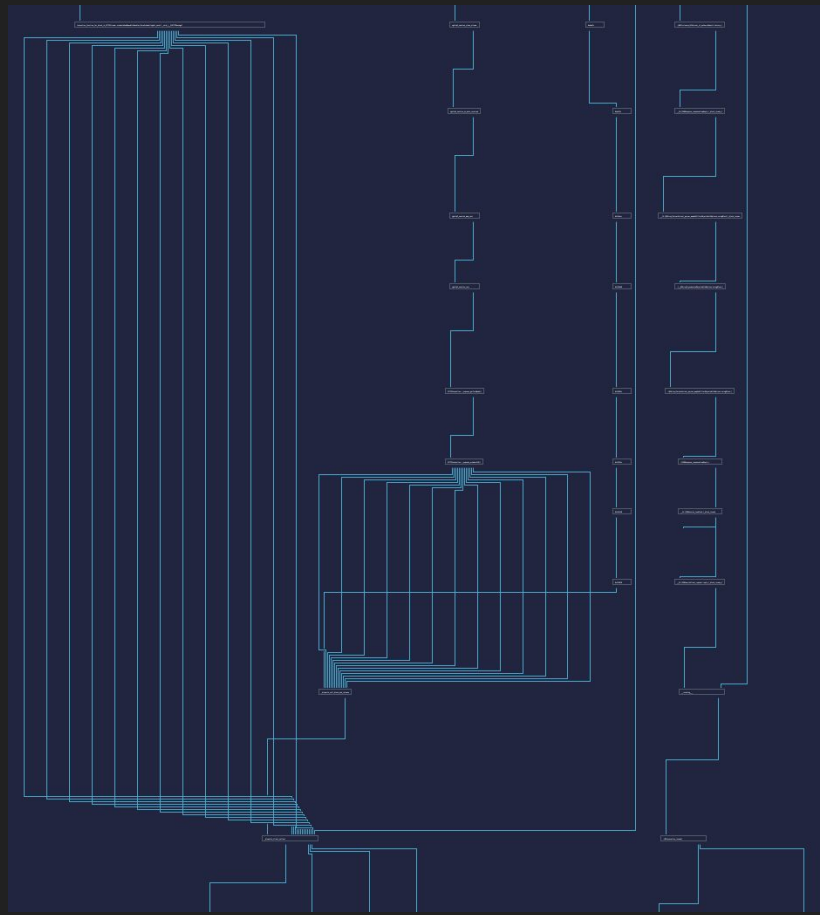
Frida support heap insecting APIs for macOS and iOS

- Yeah proper linux support is welcome here :D any contributor?
- We can easly dump all the heap from a program and carve it

Backtracing TraceGraphs

Sounds and looks cool.

- BONUS: And it's useful!



Questions?

R2 Spam - Spread the dword!

- We organize a yearly conference
  - 4 trainings + 20 talks + grapes
- I'll be giving a training at BlackHat about r2 and r2frida
- GSoC/RSoC/GSoD
- The IRC/Telegram channels with > 2000 ppl

Thanks!