BUILDING A CONCRETE ALTERNATIVE TO IDA

Radare2 to the rescue!

Jeffrey (crowell) Crowell – Julien (jvoisin) Voisin

June 21, 2015

REcon 2015 – Montreal
WE’RE SORRY
Who are we?

Crowell
- Work at Google
- raxcity.com
- Shellphish
- Boston Key Party

Jvoisin
- Soon graduated
- <redacted>
- dustri.org
- Knows some English
Professional
- IDA Pro
- ImmunityDBG
- WinDBG

Amateur
- IDA Pro
- WineDBG
- Hopper
- OllyDBG
Professional

- IDA Pro ($5000)
- ImmunityDBG
- WinDBG

Amateur

- IDA Pro (pirated)
- WineDBG (pirated Windows)
- Hopper (probably not)
- OllyDBG (not maintained)
· Created by Ilfak Guilfanov
- Created by Ilfak Guilfanov
- First DataRescue, then Hex-Rays
· Created by Ilfak Guilfanov
· First DataRescue, then Hex-Rays
· Closed-source and expensive
IDA Pro

- Created by Ilfak Guilfanov
- First DataRescue, then Hex-Rays
- Closed-source and expensive
- Lots of architectures are supported
· Created by Ilfak Guilfanov
· First DataRescue, then Hex-Rays
· Closed-source and expensive
· Lots of architectures are supported
· Decompilation!
• Created by Ilfak Guilfanov
• First DataRescue, then Hex-Rays
• Closed-source and expensive
• Lots of architectures are supported
• Decompilation!
• **Awesome** piece of software
RADARE2, CET INCONNU
HISTORY

- radare in 2006
HISTORY

- radare in 2006
- forensics tool
HISTORY

- radare in 2006
- forensics tool
- radare2 in 2009
HISTORY

- radare in 2006
- forensics tool
- radare2 in 2009
- written in pure C
HISTORY

- radare in 2006
- forensics tool
- radare2 in 2009
- written in pure C
- 350k LoC under LGPL
HISTORY

- radare in 2006
- forensics tool
- radare2 in 2009
- written in pure C
- 350k LoC under LGPL
- multi-purpose suite of tools
· likely packaged in your distribution
- likely packaged in your distribution
- install from source though ;-)
likely packaged in your distribution
install from source though ;-) 
more than 50 contributors for the latest release
- likely packaged in your distribution
- install from source though ;-)
- more than 50 contributors for the latest release
- RSoC (+GSoC)
Compile programs into tiny binaries for x86-32/64 and arm.
R2TOOLS

- ragg2
- radiff2
- rabin2
- rabin2
- rafind2
- rahash2
- rarun2
- rasm2
- rax2
- radare2

Binary diffing
R2TOOLS

- ragg2
- radiff2
- rabin2
- rafind2
- rahash2
- rarun2
- rasm2
- rax2
- radare2

Binary program info extractor (think *readelf*)
Search for byte patterns in files
R2TOOLS

- ragg2
- radiff2
- rabin2
- rafind2
- rahash2
- rarun2
- rasm2
- rax2
- radare2

Block based hashing utility
R2TOOLS

- ragg2
- radiff2
- rabin2
- rafind2
- rahash2
- rarun2
- rasm2
- rax2
- radare2

Run programs in exotic environments
<table>
<thead>
<tr>
<th>R2TOOLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ragg2</td>
</tr>
<tr>
<td>radiff2</td>
</tr>
<tr>
<td>rabin2</td>
</tr>
<tr>
<td>rafind2</td>
</tr>
<tr>
<td>rahash2</td>
</tr>
<tr>
<td>rarun2</td>
</tr>
<tr>
<td>rasm2</td>
</tr>
<tr>
<td>rax2</td>
</tr>
<tr>
<td>radare2</td>
</tr>
</tbody>
</table>

Assembler/disassembler
R2TOOLS

- ragg2
- radiff2
- rabin2
- rafind2
- rahash2
- rarun2
- rasm2
- rax2
- radare2

Base converter
Combine \textit{everything} together
## Platforms

### Runs on
- Windows
- GNU/Linux
- *BSD
- OSX
- Android and iOS
- Smartwatch
- Web browser
- QNX
- ...

### Handles
- MZ/PE+/PE/COFF
- ELF, ELF64
- Fatmach0/Mach0
- DEX/JAVA
- BIOS/TE
- GB/GBA/DS
- XBOX
- Plan9
- BIOS
<table>
<thead>
<tr>
<th>Architectures</th>
</tr>
</thead>
<tbody>
<tr>
<td>· 8051</td>
</tr>
<tr>
<td>· arc</td>
</tr>
<tr>
<td>· arm</td>
</tr>
<tr>
<td>· avr</td>
</tr>
<tr>
<td>· brainfuck</td>
</tr>
<tr>
<td>· cr16</td>
</tr>
<tr>
<td>· csr</td>
</tr>
<tr>
<td>· dalvik</td>
</tr>
<tr>
<td>· dcpu16</td>
</tr>
<tr>
<td>· ebc</td>
</tr>
<tr>
<td>· gb</td>
</tr>
<tr>
<td>· h8300</td>
</tr>
</tbody>
</table>
ARCHITECTURES

- i4004
- i8080
- java
- LH5801
- m68k
- malbolge
- mips
- msil
- msp430
- nios2
- powerpc
- rar
ARCHITECTURES

- ART
- sh
- sparc
- spc700
- sysz
- tms320
- v850
- whitespace
- x86
- xcore
- z80
- propeller
- snes
- psosvm
- 6502
R2 INTERNALS
· At it’s heart, a library.
· Swig/Valabind
· Build your own tools on top of radare2

```c
#include <r_asm.h>
#include <r_anal.h>
#include <r_types.h>
#include <stdio.h>

void main (){ 
RAsm *a;
RAsmOp *aop;
RAnal *anal;
RAnalOp *anop;
uint8 hex = 0x00;
a = r_asm_new ();
anal = r_anal_new ();
aop = R_NEW0(RAsmOp);
anop = r_anal_op_new ();
r_asm_use (a, "gb");
r_anal_use (anal, "gb");
r_anal_op (anal, anop, 0x0, &hex, 1);
r_asm_set_pc (a, 0x0);
r_asm_disassemble (a, aop, &hex, 1);
printf("0x%02x\t\ts\t\tcyclenlen is %i\n",
    hex, aop->buf_asm, anop->cycles
free (aop);
r_anal_op_free (anop);
r_asm_free (a);
r_anal_free(anal);
}
```
R2 IS A LIBRARY, WITH R2PIPE INCLUDED

[1] pry(main)> require 'r2pipe';
[2] pry(main)> r2p = R2Pipe.new '/bin/ls';
[3] pry(main)> puts r2p.cmd 'ie'; # print entrypoint

[EntryPoints]
vaddr=0x004048c5  paddr=0x000048c5  baddr=0x00400000  laddr=0x00000000

1 entrypoints

Bindings are boring, let’s call r2 instead!
R2 is pluggable

3rd party (or 1st party) plugins

- \textit{r\_asm}, assembler and disassembler
- \textit{r\_anal}, code analysis (opcode, type, esil)
- \textit{r\_reg}, registers
- \textit{r\_syscall}, system calls
- \textit{r\_debug}, debugger
- \textit{r\_io}, io layer
- \textit{r\_search}, search engine
- ...
FEATURE COMPARISON
IDA HAS A BOOK, R2 IS SELF-DOCUMENTED (AND ALSO HAS A BOOK TOO)

- R2 is like vim
- Combine *intuitives* commands
- Just append `?` everywhere
IDA HAS PLUGINS, R2 HAS MORE BINDINGS

- Python
- NodeJS
- C
- Lua
- Lisp
- Vala
- Ruby
- Go
- Rust
- Perl
- OCaml
- ...
· Minimap
· Debugger-compliant
· Interactive

IDA HAS SOME GRAPHS, R2 DOES TOO (BUT IN ASCII)
IDA IS CLEVER BUT ALSO INTERACTIVE, SO IS R2

- name functions
- mark flags
- define code/data
- leave comments
- name stack variables
- mark structures
- use types
- define/modify functions
IDA HAS A NICE GUI, SO DOES, WELL, ERR, MH, …
ACTUALLY...

It’s not all that scary!

- *Visual Mode* - friendly enough?
- Familiar vim keybindings.
- *Web UI* - The future of collaborative reversing!
- Communicate over r2pipe.
IDA HAS AN OLD-SCHOOL TUI MODE, R2 HAS A BETTER ONE.

- Ncurses-like
- Static
- Dynamic
- Analysis
- Try it, really.
IDA HAS NO WEB-UI, R2 DOES.
IDA HAS A DEBUGGER, SO DOES R2

- Classic features
- Visual mode too
- Several backends
- Tracing
- Remote
IDAGHS KICK-ASS ANALYSIS, R2 HAS SOME TOO

- Functions detection
- Local var detection
- FLIRT integration
- zignatures
- (X)REF
- DWARF and PDB
IDA SOME INTERNAL IL, R2 HAS AN OPEN ONE

- ESIL
- RPN-ish
- Documented
- Emulation
- Decompilation
- Analysis
IDA HAS PLUGINS FOR PWNAGE, R2 PUT THIS IN CORE

- Regexp ROP hunter
- Mitigations detection
- Emulation
- Patterns
- Environment control
IDA HAS PLUGINS FOR BINDIFFING, R2 PUT THIS IN CORE
SUMMARY
· GSoC
· Stabilization
· A fresh release
· Second edition of our RSoC
· ~1000 LoC modified per week
CURRENT DRAWBACKS

- Super-steep learning curve
- A lot of features
- Fast-moving target
- IDA is friendlier
CURRENT BENEFITS

- Free-software
- Exotic arch support
- Active development
- A lot of features
- More and more users

KEEP CALM AND USE RADARE2
WHO USES R2 CURRENTLY?

- Some top-notch CTF teams
  - Shellphish
  - Dragon Sector
  - ...

- Anti-malware companies
  - AlienVault
  - IOActive
  - ...

- Some popular RE projects
  - Coreboot
  - Magic lantern
  - ...

- Cool wargames
  - io from smashthestack
  - OverTheWire
  - ...
WHO USES R2 CURRENTLY?

- Some top-notch ctf teams
  - Shellphish
  - Dragon Sector
  - ...
- Anti-malware companies
  - AlienVault
  - IOActive
  - ...
- Some popular RE projects
  - Coreboot
  - Magic lantern
  - ...
- Cool wargames
  - io from smashthestack
  - OverTheWire
  - ...

We do!
Do you?
AND TOMORROW?

- Complete-emulation
- Decompilation
- A complete GUI
- What do you want?
Question IDA supremacy¹.

Monoculture is bad.

¹And don’t pirate it!
Radare2 is nice.

You should use it.¹

¹Or at least try it
RESOURCES

- TV channel - http://radare.tv/
- Book - http://maijin.gitbooks.io/radare2book/content/
- Blog - http://radare.today/
- Homepage - http://rada.re/
- Source code - http://github.com/radare/radare2/
- IRC channel - irc://irc.freenode.net/radare

Come talk to us!
Questions?