radare2
//rooted

pancake
pancake@nopcode.org

nibble
nibble.ds@gmail.com

Overview

* Full rewrite focusing on:

- API
- Portability
- Modularity
- Scripting and bindings

* Status in 0.4

- Aiming to be as compatible as possible with r1
- Some command and concepts has been redefined
- Runtime >10x faster
- Smart and cleaner code (74KLOC vs 130KLOC)

Relocatable code compiler

* Simple and minimal compiler for x86 32/64
  - arm and powerpc support will follow
  - C-like syntax, with low-level hints
  - Allows to generate assembly code ready to be injected
  - Used as interface for native and crossplatform injection
* Accessible thru shell and api

```
r_sys_cmd_str -> r_asm_massemble -> r_debug_inject
```

Language bindings

* C is fun, but people love to loose CPU cycles..
  - Automatic bindings generated by valaswig
  - Vala and Genie by default
  - Python, Perl, Lua and Ruby (more will come)
  - Access to full internal API
  - Binded code can use native instances and viceversa
* Valaswig is a .vapi to .i translator

```
$ hg clone http://hg.youterm.com/valaswig
```

Debugging API

* Several APIs affected
  - debug, reg, bp, io
  - No `os/arch` specific stuff

Demo

This is a demo:

```
$ r2 -V
radare2 0.4 @ linux-lil-x86
```

```
main() {
	printf( "Hello, World!0);
}
#define ut64 unsigned long long
#define ut8 unsigned char

static int verbose = 1;
static char *script = 0;
static ut64 oldseek, curseek = 0LL;
static int obsize, bsize = 256;
static int red_cmd(char *cmd); // XXX : recursive depenenc
#define BUFSZ 128*1024

#include "red.h"
#include "util.c"
#include "cmd.c"

static void red_slurpin() {
	ut8 buf[BUFSZ];
	for(;;) {
		int len = read(0, buf, sizeof(buf));
		if (len<1) break;
		hexdump(buf, len, 16);
		curseek += len;
	}
}
```

This is fun

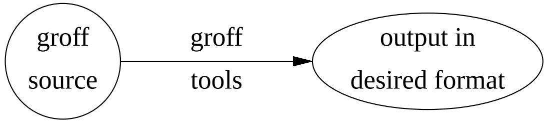
- next Point!

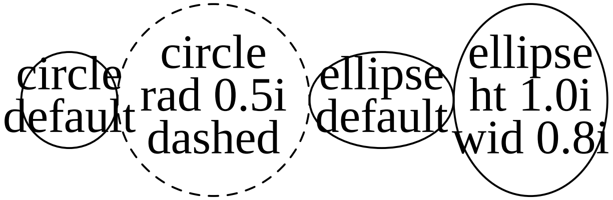
Next Slide

- next Point!

Intxxxxction

This is 32p This is 24p This is 10p





This is the title
BodBodyy

- Aiming to offer a reliable API providing radare core features
- Break the limitations for plugins and scripting language bindings

Math

$$\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\cdots}}}} = 0.6180\cdots$$