automated patching using r2

8=====D lacon2010

pancake
pancake@nopcode.org

Who am I?

Introduction

This presentation is going to show a simple tool to automatize the patch of binaries. Something like a reduced batch version of radare in few lines of C using the r2 api.

Patches are defined in a plain text file.

```
$ cp /bin/ls ls
$ rapatch ls patch.txt
$ ./ls
Hello World!
```

Where to get it?

You will need the r2 api in order to compile it

```
$ hg clone http://radare.org/hg/radare2
$ cd radare2
$ ./configure --prefix=/usr
$ make
$ sudo make symstall
```

This tool lives in radare2-extras repository.

```
$ hg clone http://radare.org/hg/radare2-extras
$ cd radare2-extras/binr/rapatch
$ make
```

File format

This is a sample rapatch script showing its features:

```
# comment
!echo Patching program
0x8048500  "Hello World"
0x8048200  223344
0x8048300  : nop;nop;nop
entry0 {
  # rarc2 integration
  printf@alias(${imp.printf});   # flag subst
  main@global(,128) {
    printf ("Hello %s", "World");
    : mov eax, 1
    : int 0x80
  }
}
```

More features?

Works for..

- Windows, Linux, OSX, iOS
- x86/x86-64/arm
- Fix vulnerabilities
- Construct new programs
  - Reusing symbols and imports
  - Writing code/data everywhere

Example

Questions?