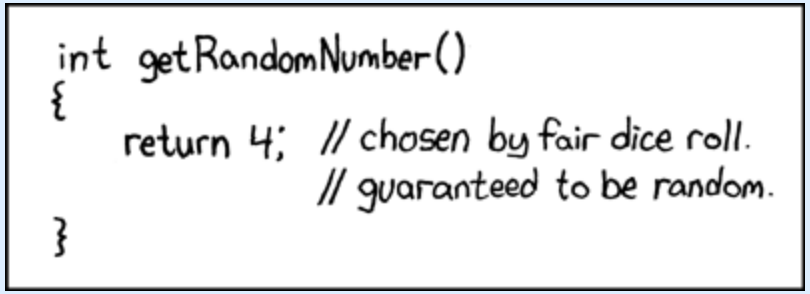
LD_PRELOAD and you

By Jesse Spielman / @heavyimage

First, xkcd.com/221



"RFC 1149.5 specifies 4 as the standard IEEE-vetted random number."

Why am I showing you this?

We're going to do it!

Why would you want to do this?

Modifying programs without recompiling them ("dynamically") rules.

Wat?

- **Environment Variables**
- the **Dyamic Linker**
- your new best friend, **LD_PRELOAD**

Background: Environment Variables

```
[jesse@carcosa:~]$ env
SHELL=/usr/local/bin/bash
XPC_FLAGS=0x0
HISTCONTROL=ignoreboth
TERM_PROGRAM_VERSION=421.2
USER=jesse
DELIGHT=/Applications/Graphics/3Delight/
TMUX=/tmp//tmux-501/default,3834,0
PKG_CONFIG_PATH=:/opt/X11/lib/pkgconfig:/opt/X11/lib/pkgconfig
...
[jesse@carcosa:~]$ echo USER
USER
[jesse@carcosa:~]$ echo $USER
jesse
```

random_num.c

```c
#include <stdio.h>
#include <stdlib.h>
#include <time.h>

int main(){
    srand(time(NULL));  // initialize RNG

    for (int i=0; i<30; i++){
        printf("%d ", rand() % 100);
    }
    printf("\n");
    return 0;
}
```

unrandom.c

```c
int rand(){
    return 4; // chosen by fair dice roll.
              // guaranteed to be random.
}
```

Get on with it!

```
$ ls
Makefile  random_num.c  unrandom.c

$ make
gcc random_num.c -o random_num
gcc -shared -fPIC unrandom.c -o unrandom.so

$ ./random_num
50 53 41 57 8 11 77 28 11 77 39 74 54 66 51 19 76 27 38 33 13 36 66 8 70 12 38 7 2 41

$ ./random_num
65 62 38 29 58 71 94 22 87 47 13 69 43 70 69 37 20 19 98 26 63 93 21 68 22 95 83 63 46 26
```

And now...

```
$ env LD_PRELOAD=$PWD/unrandom.so ./random_num
4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
```

or

```
$ export LD_PRELOAD=$PWD/unrandom.so

$ ./random_num
4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
```

W(h)at just happened?

- Dynamic linker magic:

```
[jesse@carcosa:~]$ ldd ./random_num
        linux-vdso.so.1 (0x00007ffcb4f17000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f2151d46000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f2151f36000)
```

- We happen to have `random_num`'s source but imagine if we didn't...

Conclusion

- XKCD is real
- Altering compiled programs is possible
- What ways can you imagine altering program behavior?

Related Tools:

- preeny
- frida
- Intel: Optimizing zlib
- OverrideQtSplashscreen

More info:

- LD_PRELOAD: The Hero We Need and Deserve
- The LD_PRELOAD trick
- Dynamic linker tricks: Using LD_PRELOAD to cheat, inject features and investigate programs

Thanks for listening!

Slides + code @
https://github.com/heavyimage/ld_preload_afnom_talk