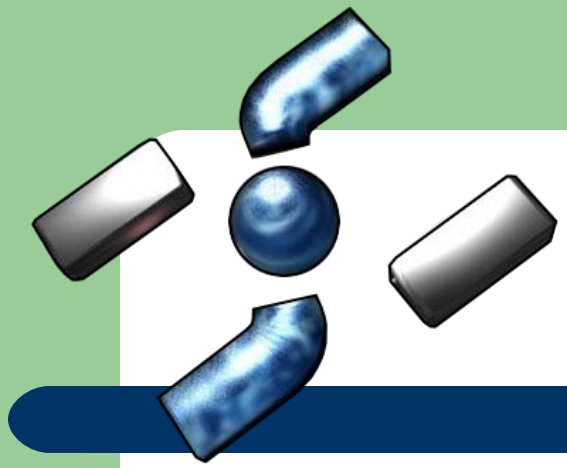
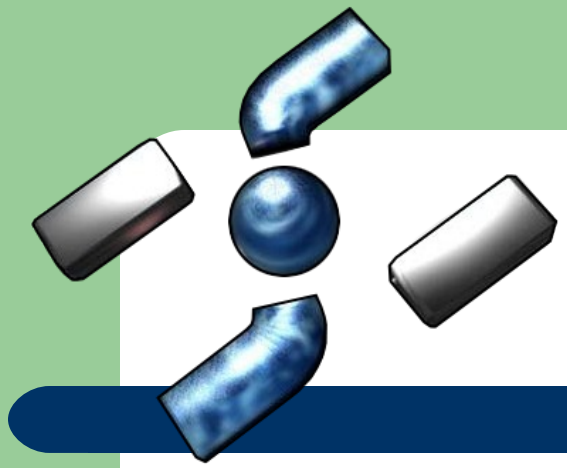


Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

- Adam Zabrocki
- http://pi3.hack.pl (nie działa ;))
- pi3@itsec.pl (lub oficjalnie: adam@hispasec.com)

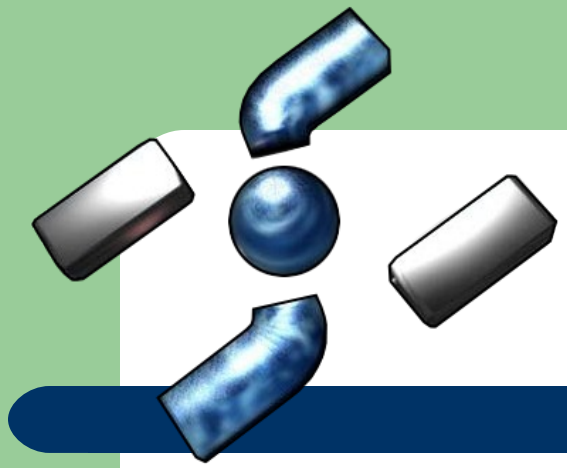


Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

- Mapa prezentacji:
  - Dla kogo wykład?

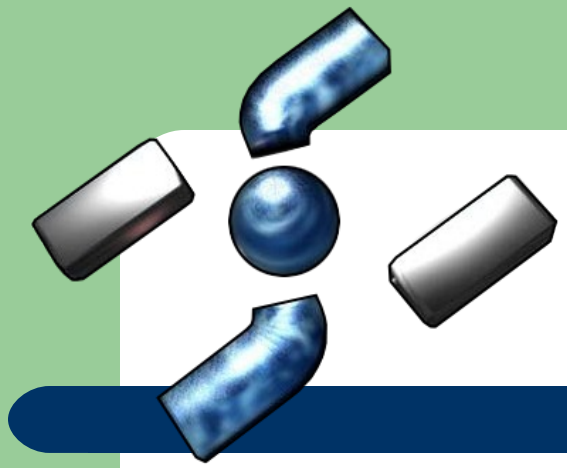


Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

- Mapa prezentacji:
  - Dla kogo wykład?
  - Cel wykładu...

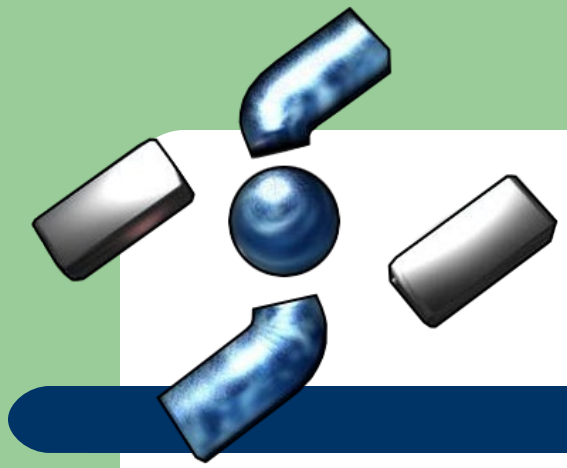


Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

- Mapa prezentacji:
  - Dla kogo wykład?
  - Cel wykładu...
  - Błędy... parę ciekawych (wg mnie) przykładów... ;-)

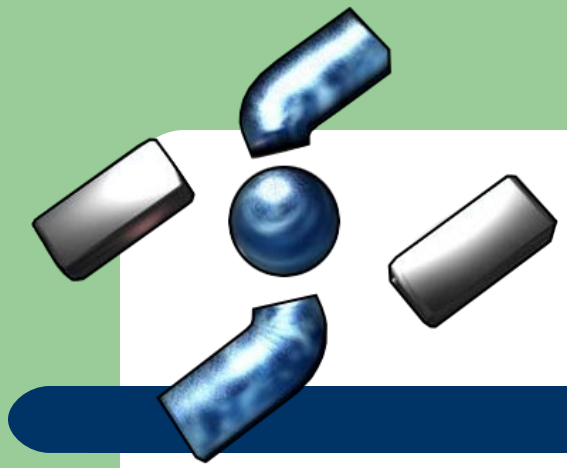


Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

- Mapa prezentacji:
  - Dla kogo wykład?
  - Cel wykładu...
  - Błędy... parę ciekawych (wg mnie) przykładów... ;-)
  - Losowe przemyślenia...



Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

- Mapa prezentacji:
  - Dla kogo wykład?

Unusual bugs

- Mapa prezentacji:
  - Dla kogo wykład?

Unusual bugs

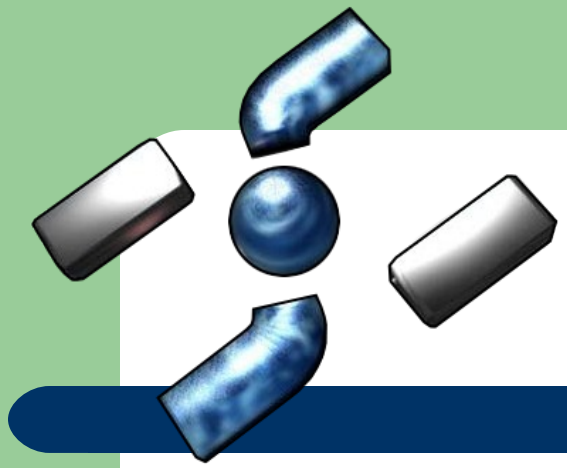
- Mapa prezentacji:
  - Dla kogo wykład?

Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

- Mapa prezentacji:
  - Dla kogo wykład?



Hispasec Sistemas

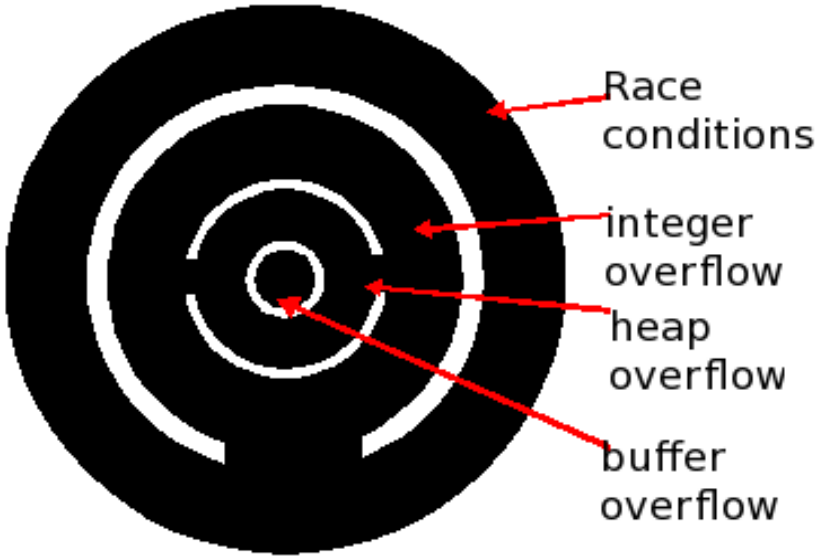
Seguridad y Tecnologías de la Información

Unusual bugs

- Mapa prezentacji:
  - Cel wykładu...

Unusual bugs

- Mapa prezentacji:
  - Cel wykładu...

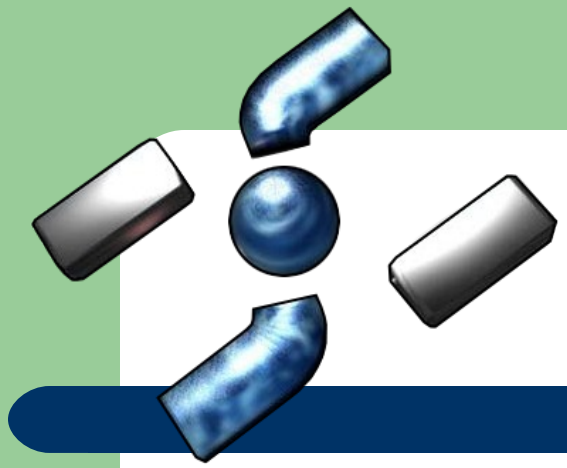


Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

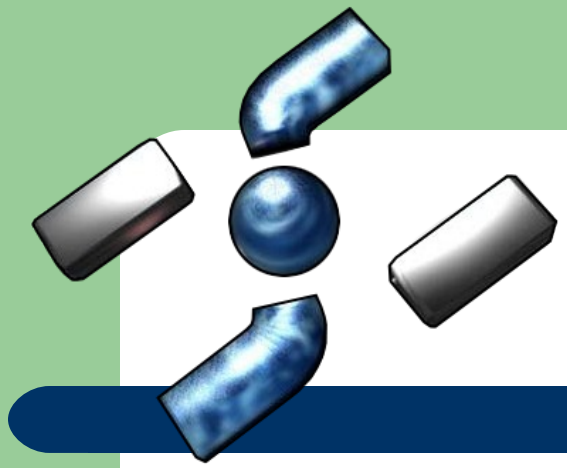
- Mapa prezentacji:
  - Cel wykładu...



Unusual bugs

- Bugs:
  - static/dynamic size of array.

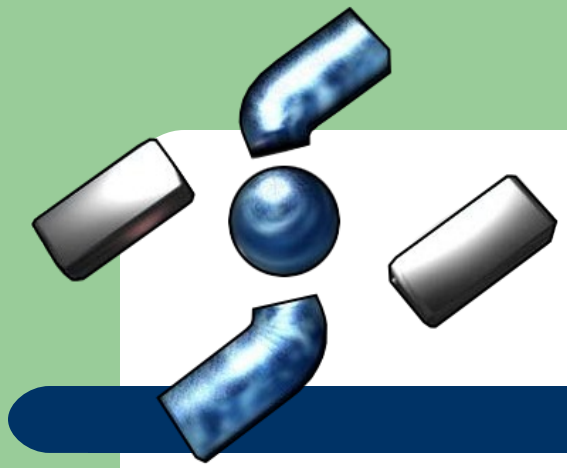
```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#define SIZE 0x10

typedef unsigned long p_type;

int main(int argc, char *argv[]) {

  p_type buf[4];
  char *ptr;

  if (argc != 2)
    exit(-1);
  memcpy(buf,argv[1],SIZE);
  ptr = (char*)&buf;
  ptr += sizeof(p_type)*4-1;
  printf("[%p - %p = %x] %s",buf,ptr,(int)ptr-(int)&buf,buf);
  return 0;
}
```



Unusual bugs

- Bugs:
  - static/dynamic size of array.

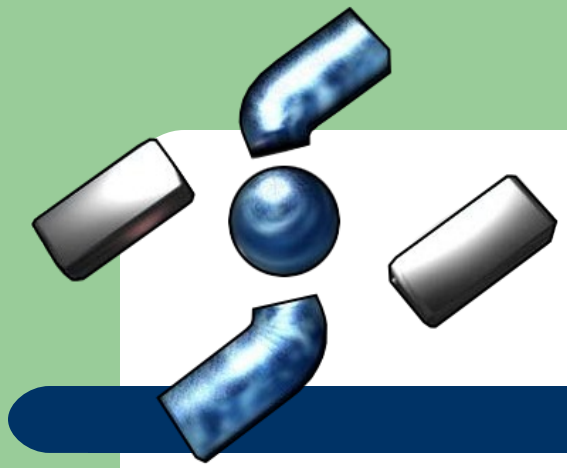
```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#define SIZE 0x10

typedef unsigned long p_type;

int main(int argc, char *argv[]) {

  p_type buf[4];
  char *ptr;

  if (argc != 2)
    exit(-1);
  memcpy(buf,argv[1],SIZE);
  ptr = (char*)&buf;
  ptr += sizeof(p_type)*4-1;
  printf("[%p - %p = %x] %s",buf,ptr,(int)ptr-(int)&buf,buf);
    return 0;
}
```



Unusual bugs

- Bugs:
  - static/dynamic size of array.

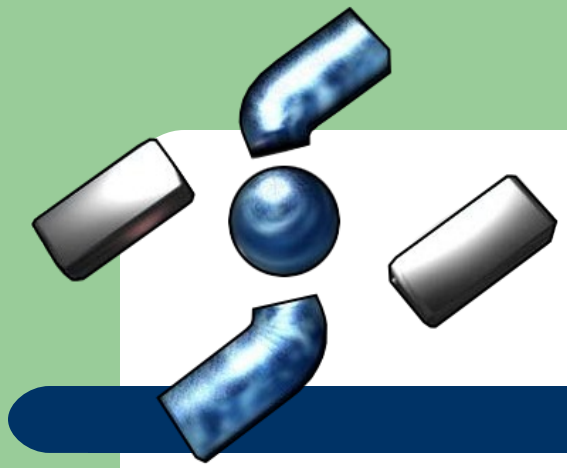
```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#define SIZE 0x10

typedef unsigned long p_type;

int main(int argc, char *argv[]) {

  p_type buf[4];
  char *ptr;

  if (argc != 2)
    exit(-1);
  memcpy(buf,argv[1],SIZE);
  ptr = (char*)&buf;
  ptr += sizeof(p_type)*4-1;
  printf("[%p - %p = %x] %s",buf,ptr,(int)ptr-(int)&buf,buf);
  return 0;
}
```



Unusual bugs

- Bugs:
  - static/dynamic size of array.

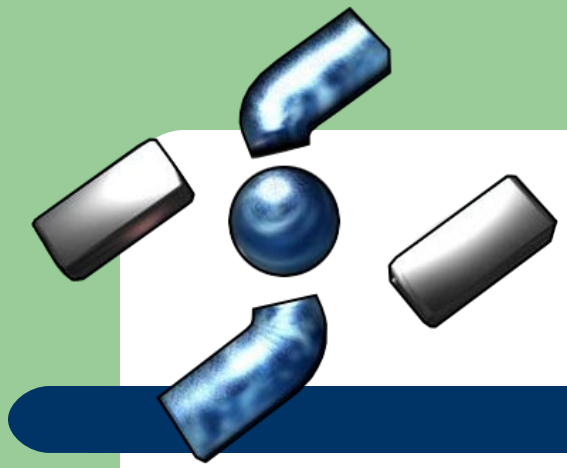
```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#define SIZE 0x10

typedef unsigned long p_type;

int main(int argc, char *argv[]) {

  p_type buf[4];
  char *ptr;

  if (argc != 2)
    exit(-1);
  memcpy(buf,argv[1],SIZE);
  ptr = (char*)&buf;
  ptr += sizeof(p_type)*4-1;
  printf("[%p - %p = %x] %s",buf,ptr,(int)ptr-(int)&buf,buf);
  return 0;
}
```



Unusual bugs

- Bugs:
  - static/dynamic size of array.

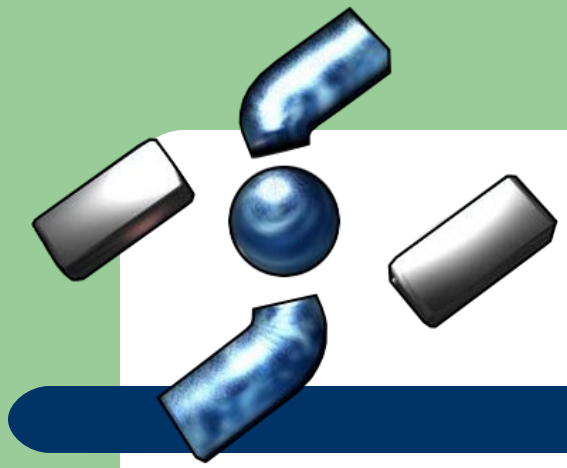
```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#define SIZE 0x10

typedef unsigned long p_type;

int main(int argc, char *argv[]) {

  p_type buf[4];
  char *ptr;

  if (argc != 2)
    exit(-1);
  memcpy(buf,argv[1],SIZE);
  ptr = (char*)&buf;
  ptr += sizeof(p_type)*4-1;
  printf("[%p - %p = %x] %s",buf,ptr,(int)ptr-(int)&buf,buf);
  return 0;
}
```



Unusual bugs

- Bugs:
  - static/dynamic size of array.

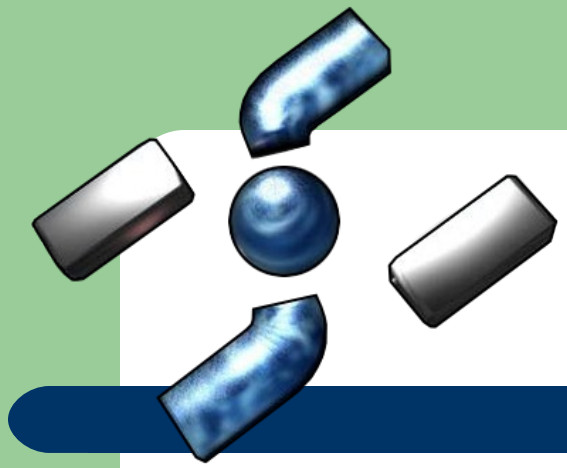
```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#define SIZE 0x10

typedef unsigned long p_type;

int main(int argc, char *argv[]) {

  p_type buf[4];
  char *ptr;

  if (argc != 2)
    exit(-1);
  memcpy(buf,argv[1],SIZE);
  ptr = (char*)&buf;
  ptr += sizeof(p_type)*4-1;
  printf("[%p - %p = %x] %s",buf,ptr,(int)ptr-(int)&buf,buf);
  return 0;
}
```



Unusual bugs

- Bugs:
  - static/dynamic size of array.

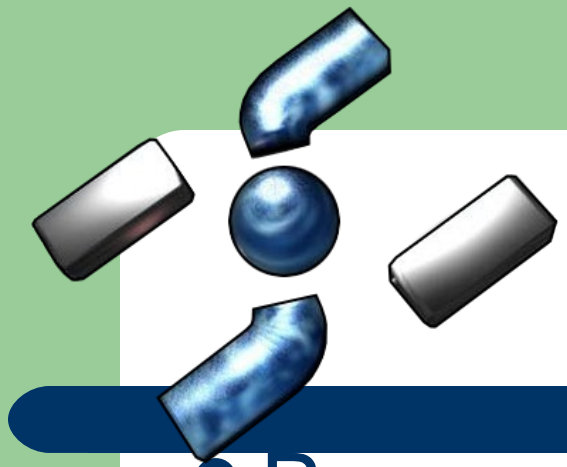
```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#define SIZE 0x10

typedef unsigned long p_type;

int main(int argc, char *argv[]) {

  p_type buf[4];
  char *ptr;

  if (argc != 2)
    exit(-1);
  memcpy(buf,argv[1],SIZE);
  ptr = (char*)&buf;
  ptr += sizeof(p_type)*4-1;
  printf("[%p - %p = %x] %s",buf,ptr,(int)ptr-(int)&buf,buf);
  return 0;
}
```



Unusual bugs

- Bugs:
  - static/dynamic size of array.

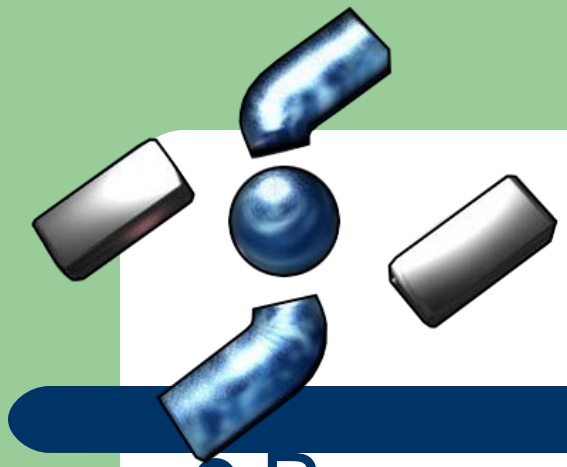
```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#define SIZE 0x10

typedef unsigned long p_type;

int main(int argc, char *argv[]) {

  p_type buf[4];
  char *ptr;

  if (argc != 2)
    exit(-1);
  memcpy(buf,argv[1],SIZE);
  ptr = (char*)&buf;
  ptr += sizeof(p_type)*4-1;
  printf("[%p - %p = %x] %s",buf,ptr,(int)ptr-(int)&buf,buf);
  return 0;
}
```



Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (32 bits)

```
[root@pi3book Secday]# gdb -q ./1
(no debugging symbols found)
(gdb) disass main
Dump of assembler code for function main:
0x08048404 <main+0>:        lea    0x4(%esp),%ecx
0x08048408 <main+4>:        and    $0xfffffff0,%esp
0x0804840b <main+7>:        pushl  -0x4(%ecx)
0x0804840e <main+10>:    push   %ebp
0x0804840f <main+11>:       mov    %esp,%ebp
0x08048411 <main+13>:    push   %ecx
0x08048412 <main+14>:    sub    $0x44,%esp
```



Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (32 bits)

```
0x0804845b <main+87>:    movb   $0x0,(%eax)
...
0x08048490 <main+140>:   add    $0x44,%esp
0x08048493 <main+143>:   pop    %ecx
0x08048494 <main+144>:   pop    %ebp
0x08048495 <main+145>:   lea    -0x4(%ecx),%esp
0x08048498 <main+148>:   ret
End of assembler dump.
(gdb) b *0x0804845b
Breakpoint 1 at 0x804845b
(gdb) b *0x08048495
```

Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (32 bits)

```
0x0804845b <main+87>:    movb   $0x0,(%eax)
...
0x08048490 <main+140>:   add    $0x44,%esp
0x08048493 <main+143>:   pop    %ecx
0x08048494 <main+144>:   pop    %ebp
0x08048495 <main+145>:   lea    -0x4(%ecx),%esp
0x08048498 <main+148>:   ret
End of assembler dump.
(gdb) b *0x0804845b
Breakpoint 1 at 0x804845b
(gdb) b *0x08048495
```

Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (32 bits)

```
(gdb) r `perl -e 'print "A"x900'`
Starting program: /media/truecrypt1/Prezentacje/Secday/1 `perl -e 'print "A"x900'`
(no debugging symbols found)
(no debugging symbols found)
(no debugging symbols found)

Breakpoint 1, 0x0804845b in main ()
(gdb) i r eax
eax            0xbffff0df   -1073745697
```

Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (32 bits)

```
(gdb) x/20x $eax-20
0xbffff0cb:    0x0482ecbf    0x41414108    0x41414141    0x41414141
0xbffff0db:    0x41414141    0xfff0df41    0xfff100bf    0xfff158bf
0xbffff0eb:    0xaed6e5bf    0x0484b000    0x04835008    0xfff15808
0xbffff0fb:    0xaed6e5bf    0x00000200    0xfff18400    0xfff190bf
0xbffff10b:    0xfe22d8bf    0x000001b7    0x00000100    0x00000000
(gdb) x/x $eax
0xbffff0df:    0xfff0df41
(gdb) c
Continuing.
Breakpoint 2, 0x08048495 in main ()
```

Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (32 bits)

```
(gdb) x/20x $eax-20
0xbffff0cb:  0x0482ecbf  0x41414108  0x41414141  0x41414141
0xbffff0db:  0x41414141  0xfff0df41  0xfff100bf  0xfff158bf
0xbffff0eb:  0xaed6e5bf  0x0484b000  0x04835008  0xfff15808
0xbffff0fb:  0xaed6e5bf  0x00000200  0xfff18400  0xfff190bf
0xbffff10b:  0xfe22d8bf  0x000001b7  0x00000100  0x00000000
(gdb) x/x $eax
0xbffff0df:  0xfff0df41
(gdb) c
Continuing.
Breakpoint 2, 0x08048495 in main ()
```

Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (32 bits)

```
(gdb) x/x 0xbffff0df
0xbffff0df:     0xfff0df00
(gdb) x/20x 0xbffff0cb
0xbffff0cb:  0x0482ecbf  0x41414108  0x41414141  0x41414141
0xbffff0db:  0x41414141  0xfff0df00  0xfff100bf  0xfff158bf
0xbffff0eb:  0xaed6e5bf  0x0484b000  0x04835008  0xfff15808
0xbffff0fb:  0xaed6e5bf  0x00000200  0xfff18400  0xfff190bf
0xbffff10b:  0xfe22d8bf  0x000001b7  0x00000100  0x00000000
(gdb) c
Continuing.
[0xbffff0d0 - 0xbffff0df = f] AAAAAAAAAAAAAAA
```

Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (32 bits)

```
(gdb) x/x 0xbffff0df
0xbffff0df:     0xfff0df00
(gdb) x/20x 0xbffff0cb
0xbffff0cb:  0x0482ecbf  0x41414108  0x41414141  0x41414141
0xbffff0db:  0x41414141  0xfff0df00  0xfff100bf  0xfff158bf
0xbffff0eb:  0xaed6e5bf  0x0484b000  0x04835008  0xfff15808
0xbffff0fb:  0xaed6e5bf  0x00000200  0xfff18400  0xfff190bf
0xbffff10b:  0xfe22d8bf  0x000001b7  0x00000100  0x00000000
(gdb) c
Continuing.
[0xbffff0d0 - 0xbffff0df = f] AAAAAAAAAAAAAAA
```

Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (64 bits)

```
0x0000000000040055c <main+0>:     push   %rbp
0x0000000000040055d <main+1>:     mov    %rsp,%rbp
0x0000000000400560 <main+4>:      sub    $0x40,%rsp
...
0x00000000004005a5 <main+73>:     movb   $0x0,(%rax)
...
0x00000000004005cf <main+115>:    callq  0x400428 <printf@plt>
0x00000000004005d4 <main+120>:    mov    $0x0,%eax
0x00000000004005d9 <main+125>:    leaveq
0x00000000004005da <main+126>:    retq
```

Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (64 bits)

```
0x0000000000040055c <main+0>:     push   %rbp
0x0000000000040055d <main+1>:          mov    %rsp,%rbp
0x0000000000400560 <main+4>:           sub    $0x40,%rsp
...
0x00000000004005a5 <main+73>:     movb   $0x0,(%rax)
...
0x00000000004005cf <main+115>:    callq  0x400428 <printf@plt>
0x00000000004005d4 <main+120>:    mov    $0x0,%eax
0x00000000004005d9 <main+125>:    leaveq
0x00000000004005da <main+126>:    retq
```

Unusual bugs

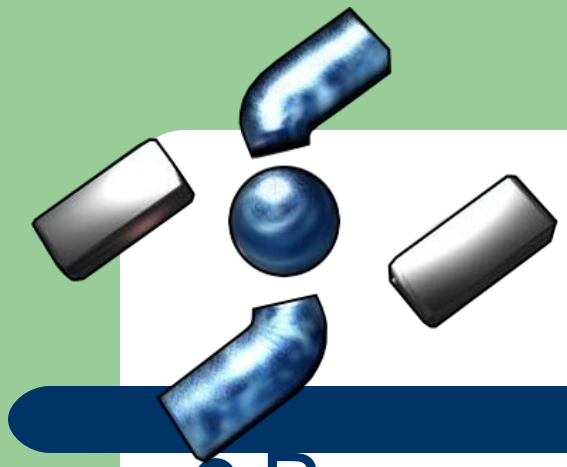
- Bugs:
  - static/dynamic size of array – debug (64 bits)

```
0x0000000000040055c <main+0>:     push   %rbp
0x0000000000040055d <main+1>:          mov    %rsp,%rbp
0x0000000000400560 <main+4>:           sub    $0x40,%rsp
...
0x00000000004005a5 <main+73>:     movb   $0x0,(%rax)
...
0x00000000004005cf <main+115>:    callq  0x400428 <printf@plt>
0x00000000004005d4 <main+120>:    mov    $0x0,%eax
0x00000000004005d9 <main+125>:    leaveq
0x00000000004005da <main+126>:    retq
```

Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (64 bits)

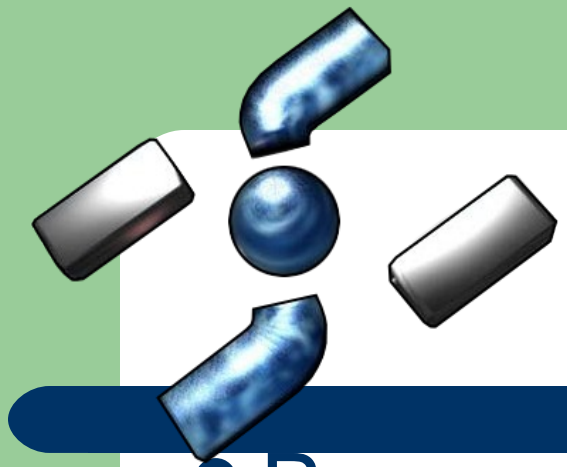
```
Breakpoint 1, 0x00000000004005a5 in main ()
(gdb) i r rax
rax            0x7fffffffe28f 140737488347791
(gdb) x/x 0x7fffffffe28f
0x7fffffffe28f: 0xffe37000
(gdb) x/20x $rax-0x20
0x7fffffffe26f: 0x41414100  0x41414141  0x41414141  0x41414141
0x7fffffffe27f: 0x00000041  0x00000000  0x40047000  0x00000000
0x7fffffffe28f: 0xffe37000  0x007fffff  0xffe28f00  0x007fffff
0x7fffffffe29f: 0x00000000  0x00000000  0x01e57600  0x000034d0
0x7fffffffe2af: 0x00000000  0x00000000  0xffe37800  0x007fffff
```



Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (64 bits)

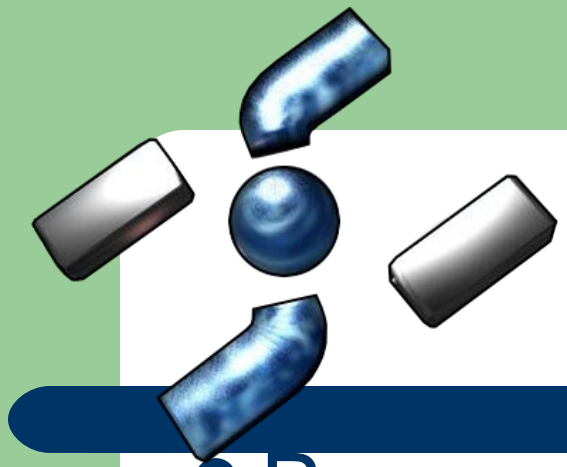
```
Breakpoint 1, 0x00000000004005a5 in main ()
(gdb) i r rax
rax            0x7fffffffe28f 140737488347791
(gdb) x/x 0x7fffffffe28f
0x7fffffffe28f: 0xffe37000
(gdb) x/20x $rax-0x20
0x7fffffffe26f: 0x41414100  0x41414141  0x41414141  0x41414141
0x7fffffffe27f: 0x00000041  0x00000000  0x40047000  0x00000000
0x7fffffffe28f: 0xffe37000  0x007fffff  0xffe28f00  0x007fffff
0x7fffffffe29f: 0x00000000  0x00000000  0x01e57600  0x000034d0
0x7fffffffe2af: 0x00000000  0x00000000  0xffe37800  0x007fffff
```



Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (64 bits)

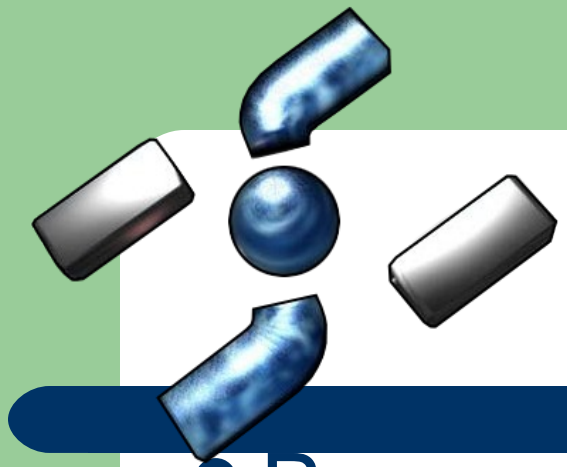
```
Breakpoint 1, 0x00000000004005a5 in main ()
(gdb) i r rax
rax            0x7fffffffe28f 140737488347791
(gdb) x/x 0x7fffffffe28f
0x7fffffffe28f: 0xffe37000
(gdb) x/20x $rax-0x20
0x7fffffffe26f: 0x41414100  0x41414141  0x41414141  0x41414141
0x7fffffffe27f: 0x00000041  0x00000000  0x40047000  0x00000000
0x7fffffffe28f: 0xffe37000  0x007fffff  0xffe28f00  0x007fffff
0x7fffffffe29f: 0x00000000  0x00000000  0x01e57600  0x000034d0
0x7fffffffe2af: 0x00000000  0x00000000  0xffe37800  0x007fffff
```



Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (64 bits)

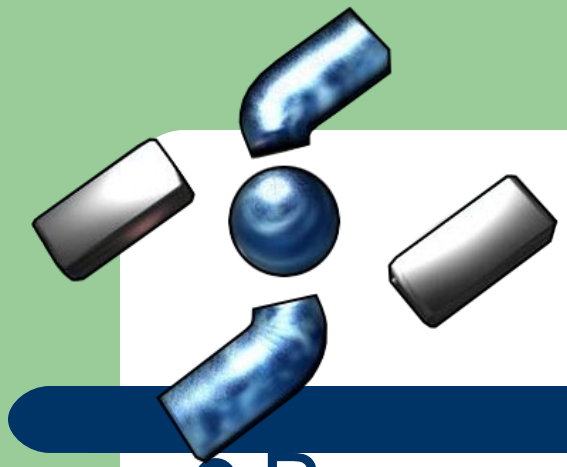
```
Breakpoint 1, 0x00000000004005a5 in main ()
(gdb) i r rax
rax            0x7fffffffe28f 140737488347791
(gdb) x/x 0x7fffffffe28f
0x7fffffffe28f: 0xffe37000
(gdb) x/20x $rax-0x20
0x7fffffffe26f: 0x41414100  0x41414141  0x41414141  0x41414141
0x7fffffffe27f: 0x00000041  0x00000000  0x40047000  0x00000000
0x7fffffffe28f: 0xffe37000  0x007fffff  0xffe28f00  0x007fffff
0x7fffffffe29f: 0x00000000  0x00000000  0x01e57600  0x000034d0
0x7fffffffe2af: 0x00000000  0x00000000  0xffe37800  0x007fffff
```



Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (64 bits)

```
(gdb) set *(0x7fffffffe27f) = 0xAABBCCDD
(gdb) set *(0x7fffffffe28f) = 0xffe370AA
(gdb) x/x 0x7fffffffe28f
0x7fffffffe28f: 0xffe370aa
(gdb) c
Breakpoint 2, 0x00000000004005cf in main ()
(gdb) x/x 0x7fffffffe28f
0x7fffffffe28f: 0xffe37000
(gdb) c
[0x7fffffffe270 - 0x7fffffffe28f = 1f] AAAAAAAAAAAAAAA
```



Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (64 bits)

(gdb) set *(0x7fffffffe27f) = 0xAABBCCDD

(gdb) set *(0x7fffffffe28f) = **0xffe370AA**

(gdb) x/x 0x7fffffffe28f

0x7fffffffe28f: 0xffe370aa

(gdb) c

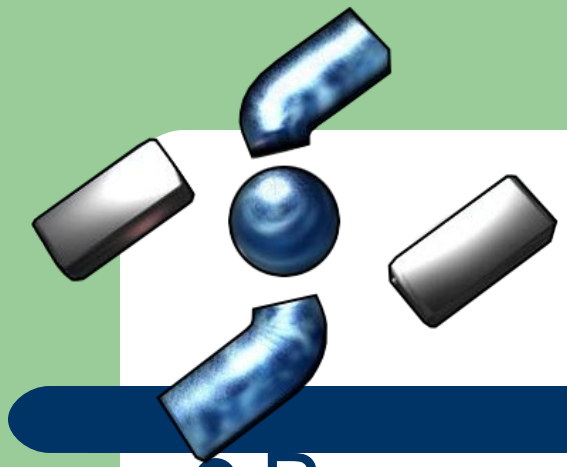
Breakpoint 2, 0x00000000004005cf in main ()

(gdb) x/x 0x7fffffffe28f

0x7fffffffe28f: 0xffe37000

(gdb) c

[0x7fffffffe270 - 0x7fffffffe28f = 1f] AAAAAAAAAAAAAAA



Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (64 bits)

(gdb) set *(0x7fffffffe27f) = 0xAABBCCDD

(gdb) set *(0x7fffffffe28f) = **0xffe370AA**

(gdb) x/x 0x7fffffffe28f

0x7fffffffe28f: **0xffe370aa**

(gdb) c

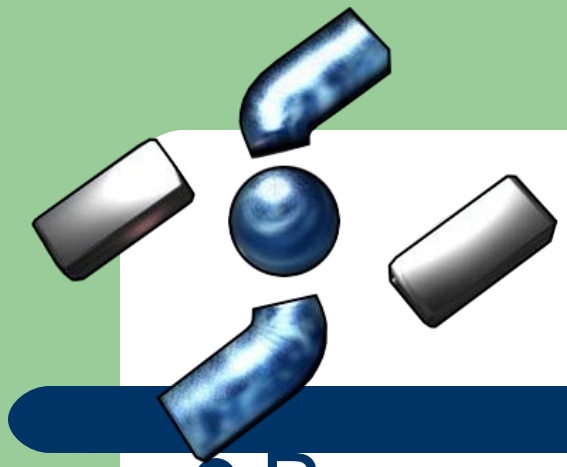
Breakpoint 2, 0x00000000004005cf in main ()

(gdb) x/x 0x7fffffffe28f

0x7fffffffe28f: 0xffe37000

(gdb) c

[0x7fffffffe270 - 0x7fffffffe28f = 1f] AAAAAAAAAAAAAAA



Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (64 bits)

(gdb) set *(0x7fffffffe27f) = 0xAABBCCDD

(gdb) set *(0x7fffffffe28f) = **0xffe370AA**

(gdb) x/x 0x7fffffffe28f

0x7fffffffe28f: **0xffe370aa**

(gdb) c

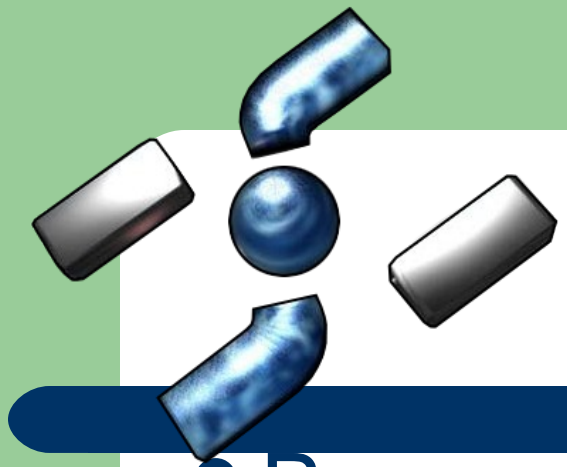
Breakpoint 2, 0x00000000004005cf in main ()

(gdb) x/x 0x7fffffffe28f

0x7fffffffe28f: **0xffe37000**

(gdb) c

[0x7fffffffe270 - 0x7fffffffe28f = 1f] AAAAAAAAAAAAAAA



Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (64 bits)

(gdb) set *(0x7fffffffe27f) = 0xAABBCCDD

(gdb) set *(0x7fffffffe28f) = **0xffe370AA**

(gdb) x/x 0x7fffffffe28f

0x7fffffffe28f: **0xffe370aa**

(gdb) c

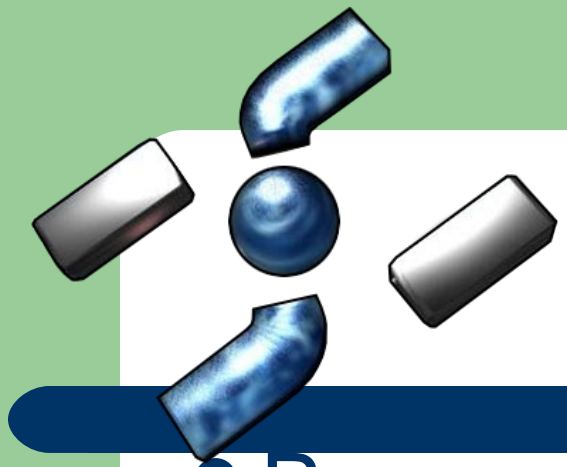
Breakpoint 2, 0x00000000004005cf in main ()

(gdb) x/x 0x7fffffffe28f

0x7fffffffe28f: **0xffe37000**

(gdb) c

[0x7fffffffe270 - 0x7fffffffe28f = 1f] AAAAAAAAAAAAAAA



Unusual bugs

- Bugs:
  - static/dynamic size of array – debug (64 bits)

(gdb) set *(0x7fffffffe27f) = 0xAABBCCDD

(gdb) set *(0x7fffffffe28f) = **0xffe370AA**

(gdb) x/x 0x7fffffffe28f

0x7fffffffe28f: **0xffe370aa**

(gdb) c

Breakpoint 2, 0x00000000004005cf in main ()

(gdb) x/x 0x7fffffffe28f

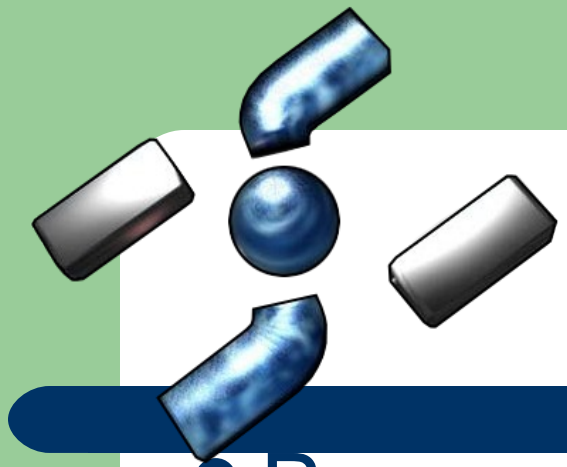
0x7fffffffe28f: **0xffe37000**

(gdb) c

[0x7fffffffe270 - 0x7fffffffe28f = **1f**] AAAAAAAAAAAAAAA

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:



Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache:

```
...
#define SOME_SIZE 64
...
typedef unsigned long AP_SOME_TYPE;
...
typedef struct {
    ...
    AP_SOME_TYPE some_array[16];
    ...
} AP_SOME_OTHER_TYPE;
```

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache:

```
...
#define SOME_SIZE 64
...
typedef unsigned long AP_SOME_TYPE;
...
typedef struct {
    ...
    AP_SOME_TYPE some_array[16];
    ...
} AP_SOME_OTHER_TYPE;
```

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache:

```
...
#define SOME_SIZE 64
...
typedef unsigned long AP_SOME_TYPE;
...
typedef struct {
    ...
    AP_SOME_TYPE some_array[16];
    ...
} AP_SOME_OTHER_TYPE;
```

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache:

...

#define SOME_SIZE 64

...

typedef unsigned long AP_SOME_TYPE;

...

typedef struct {

    ...

    AP_SOME_TYPE some_array[16]

    ...

} AP_SOME_OTHER_TYPE;

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache:

...

AP_SOME_OTHER_TYPE *ptr;

...

...

memcpy(ptr->some_array,source,SOME_SIZE);

...

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache:

...

AP_SOME_OTHER_TYPE *ptr;

...

...

memcpy(ptr->some_array,source,SOME_SIZE);

...

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache:

...

AP_SOME_OTHER_TYPE *ptr;

...

...

memcpy(**ptr->some_array**,source,SOME_SIZE);

...

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache:

...

AP_SOME_OTHER_TYPE *ptr;

...

...

memcpy(ptr->some_array,source,**SOME_SIZE**);

...

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache – konsekwencje?

32 bitowa architektura:

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache – konsekwencje?

32 bitowa architektura:

sizeof(unsigned long) = 4, wiec 16*4 = 64

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache – konsekwencje?

32 bitowa architektura:

sizeof(unsigned long) = 4, wiec 16*4 = 64

memcpy() kopiuje dokładnie taką ilość danych ile trzeba

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache – konsekwencje?

32 bitowa architektura:

sizeof(unsigned long) = 4, wiec 16*4 = 64

memcpy() kopiuje dokładnie taką ilość danych ile trzeba

64 bitowa architektura:

Unusual bugs

- Bugs:
  - static/dynamic size of array – real world:

Apache – konsekwencje?

32 bitowa architektura:

sizeof(unsigned long) = 4, wiec 16*4 = 64

memcpy() kopiuje dokładnie taką ilość danych ile trzeba

64 bitowa architektura:

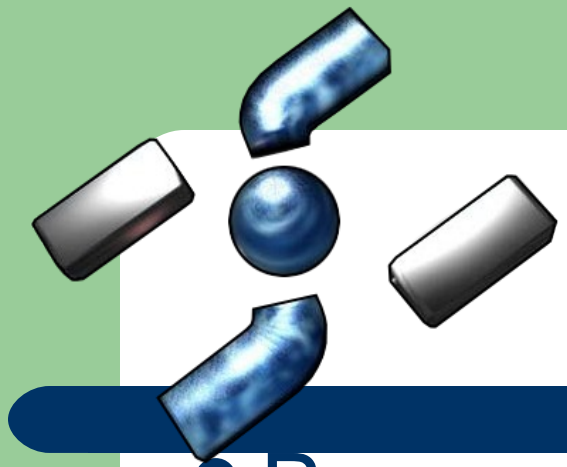
sizeof(unsigned long) = 8, wiec 16*8 = 128

memcpy() zapełnia tylko polowe tablicy, pozostała polowa jest losowa (information disclosure), a każda manipulacja na tablicy jest nieprzewidywalna

Unusual bugs

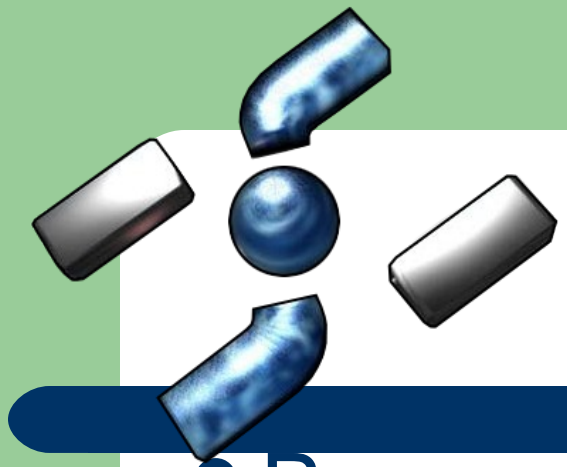
- Bugs:
  - static/dynamic size of array – real world:

Smile



Unusual bugs

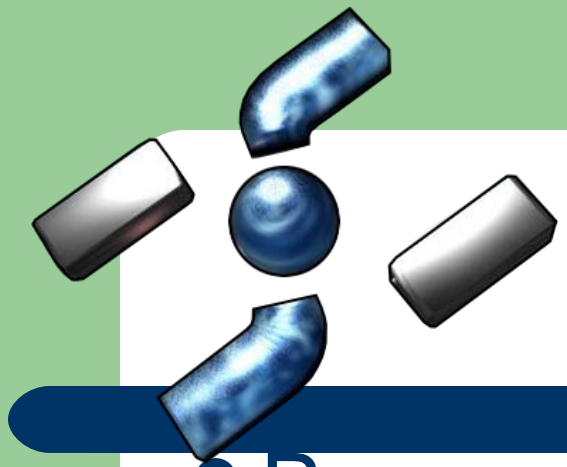
- Bugs:
  - Padding attack:



Unusual bugs

- Bugs:
  - Padding attack:

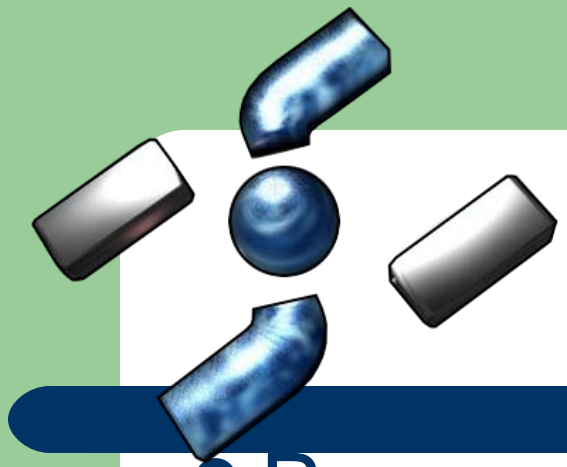
```
struct {

    int a;
    short b;
    char c;

} mama;
```



Unusual bugs

- Bugs:
  - Padding attack:

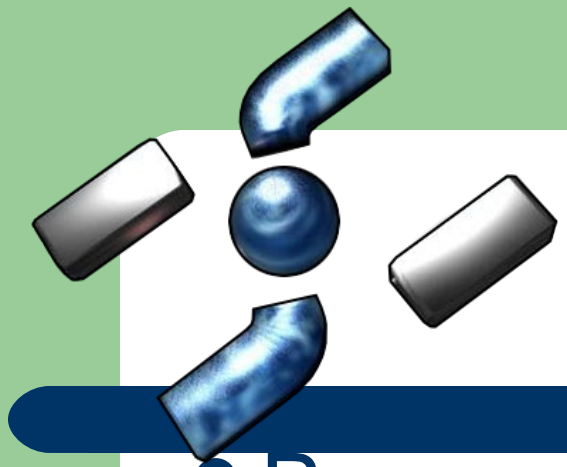
```
struct {
    int a;
    short b;
    char c;
} mama;

int main(void) {
    printf("sizeof(a)[%d]+sizeof(b)[%d]+sizeof(c)[%d] =\
     %d\n",sizeof(mama.a),sizeof(mama.b),\
    sizeof(mama.c),sizeof(mama.a)+sizeof(mama.b)\
    +sizeof(mama.c));
    printf("sizeof(mama) = %d\n",sizeof(mama));
}
```



Unusual bugs

- Bugs:
  - Padding attack:

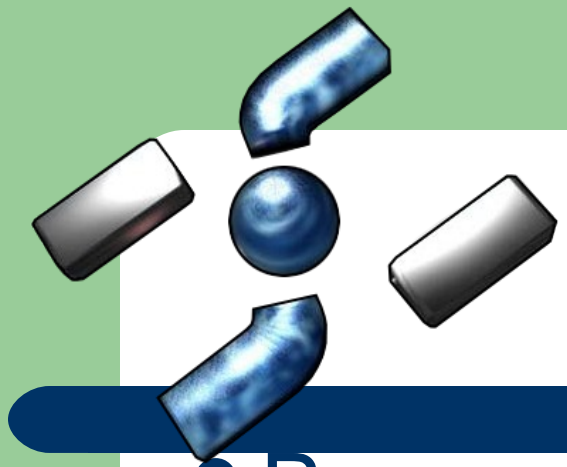
```
[root@pi3book Secday]# ./padding
sizeof(a)[4]+sizeof(b)[2]+sizeof(c)[1] = 7
sizeof(mama) = 8
```



Unusual bugs

- Bugs:
  - Padding attack:

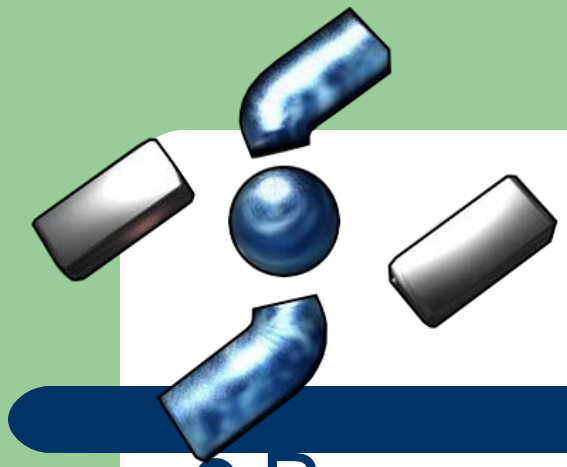
```
[root@pi3book Secday]# ./padding
sizeof(a)[4]+sizeof(b)[2]+sizeof(c)[1] = 7
sizeof(mama) = 8
```



Unusual bugs

- Bugs:
  - Padding attack:

```
[root@pi3book Secday]# ./padding
sizeof(a)[4]+sizeof(b)[2]+sizeof(c)[1] = 7
sizeof(mama) = 8
```



Hispasec Sistemas

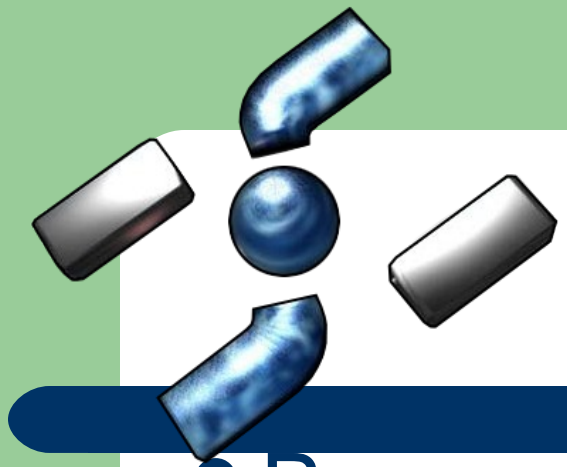
Seguridad y Tecnologías de la Información

Unusual bugs

- Bugs:
  - Padding attack:

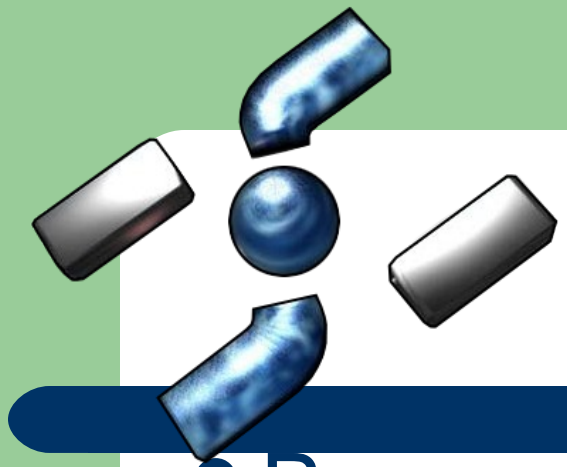
```
[root@pi3book Secday]# ./padding
sizeof(a)[4]+sizeof(b)[2]+sizeof(c)[1] = 7
sizeof(mama) = 8
```

Poważne **KONSEKWENCJE !!!**



Unusual bugs

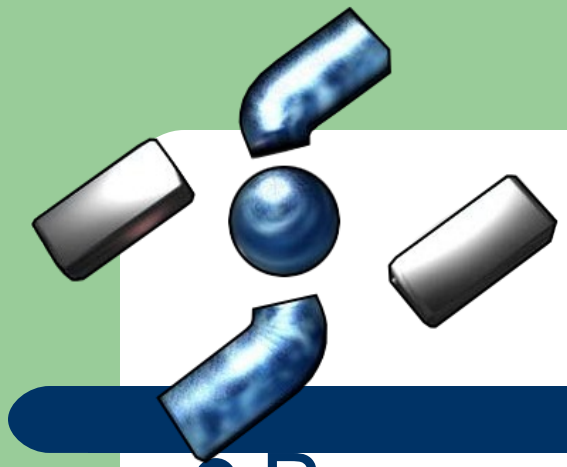
- Bugs:
  - Padding attack – real world:



Unusual bugs

- Bugs:
  - Padding attack – real world:

Linux Kernel 4-byte Information Leak (<= 2.6.31-rc5) – amd64 (x86_64):



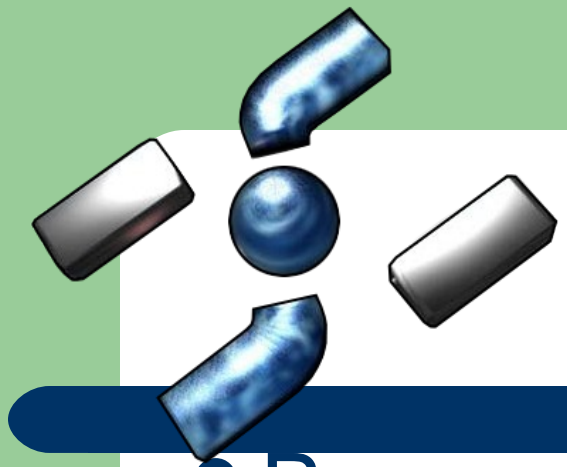
Unusual bugs

- Bugs:
  - Padding attack – real world:

Linux Kernel 4-byte Information Leak (<= 2.6.31-rc5) – amd64 (x86_64):

```
typedef struct sigaltstack {
        void __user *ss_sp;
        int ss_flags;
        size_t ss_size;
} stack_t;
```

size_t => unsigned long



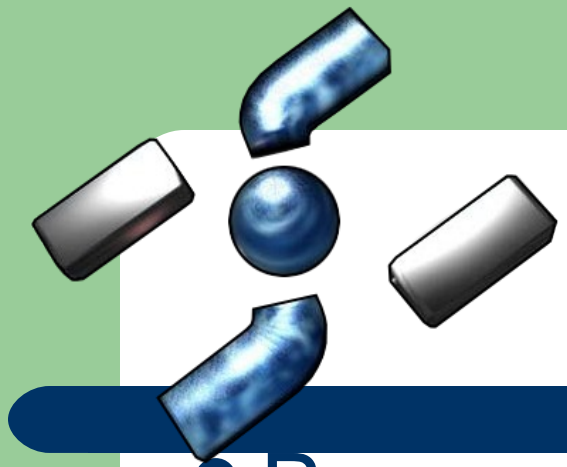
Unusual bugs

- Bugs:
  - Padding attack – real world:

Linux Kernel 4-byte Information Leak (<= 2.6.31-rc5) – amd64 (x86_64):

"kernel/signal.c"

```
int  do_sigaltstack (const stack_t __user *uss, stack_t __user *uoss, unsigned long sp){
        stack_t oss;
        int error;
          if (uoss) {
                oss.ss_sp = (void __user *) current->sas_ss_sp;
                oss.ss_size = current->sas_ss_size;
                oss.ss_flags = sas_ss_flags(sp);
        }
```



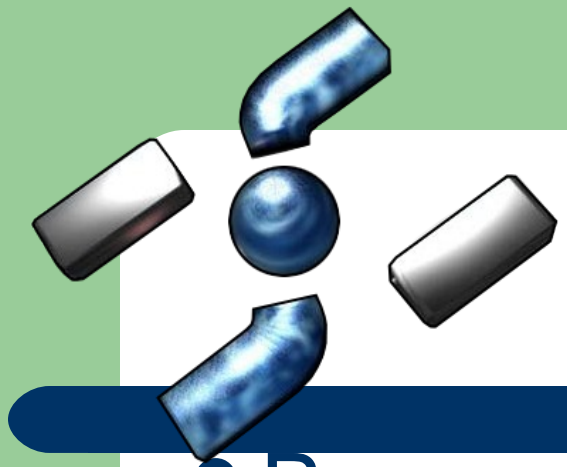
Unusual bugs

- Bugs:
  - Padding attack – real world:

Linux Kernel 4-byte Information Leak (<= 2.6.31-rc5) – amd64 (x86_64):

"kernel/signal.c"

```
int  do_sigaltstack (const stack_t __user *uss, stack_t __user *uoss, unsigned long sp){
        stack_t oss;
        int error;
          if (uoss) {
                oss.ss_sp = (void __user *) current->sas_ss_sp;
                oss.ss_size = current->sas_ss_size;
                oss.ss_flags = sas_ss_flags(sp);
        }
```



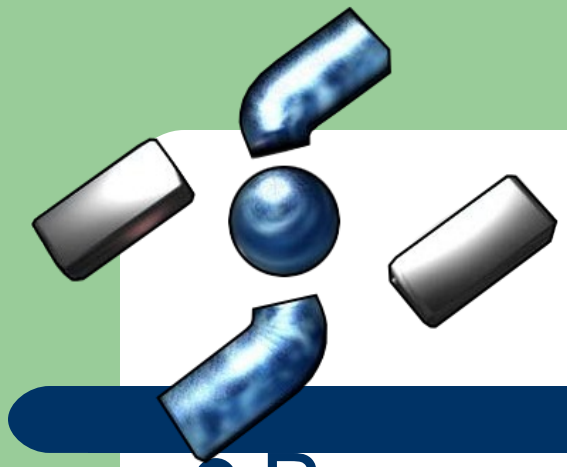
Unusual bugs

- Bugs:
  - Padding attack – real world:

Linux Kernel 4-byte Information Leak (<= 2.6.31-rc5) – amd64 (x86_64):

"kernel/signal.c"

```
int  do_sigaltstack (const stack_t __user *uss, stack_t __user *uoss, unsigned long sp){
        stack_t oss;
        int error;
          if (uoss) {
                oss.ss_sp = (void __user *) current->sas_ss_sp;
                oss.ss_size = current->sas_ss_size;
                oss.ss_flags = sas_ss_flags(sp);
        }
```

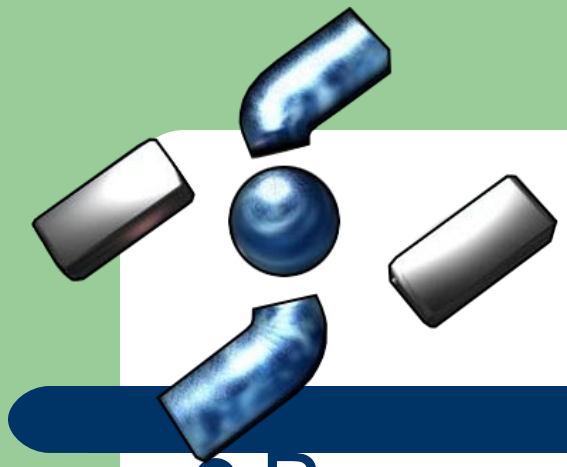


Unusual bugs

- Bugs:
  - Padding attack – real world:

Linux Kernel 4-byte Information Leak (<= 2.6.31-rc5) – amd64 (x86_64):

```
...
 if (uss) {
        void __user *ss_sp;
        ...
 }
 if (uoss) {
        error = -EFAULT;
        if (copy_to_user(uoss, &oss, sizeof(oss)))
               goto out;
 }
```



Unusual bugs

- Bugs:
  - Padding attack – real world:

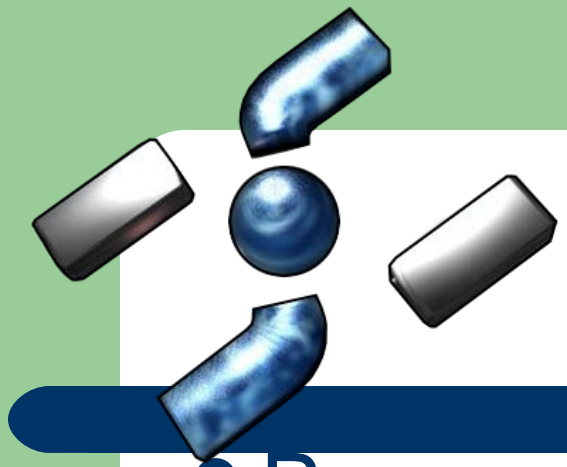
Linux Kernel 4-byte Information Leak (<= 2.6.31-rc5) – amd64 (x86_64):

```
...
 if (uss) {
        void __user *ss_sp;
        ...
 }
 if (uoss) {
        error = -EFAULT;
        if (copy_to_user(uoss, &oss, sizeof(oss)))
               goto out;
 }
```

Unusual bugs

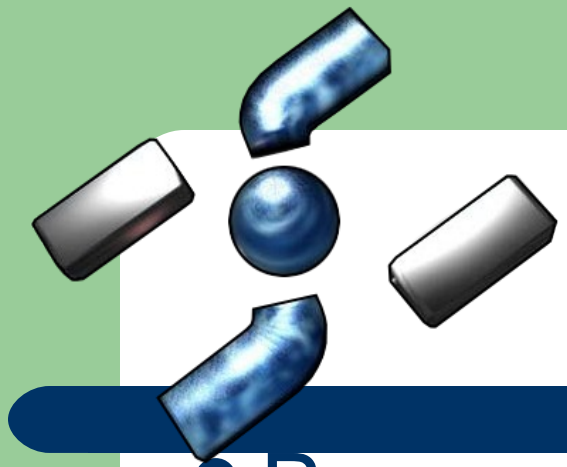
- Bugs:
  - Padding attack – real world:

Linux Kernel 4-byte Information Leak (<= 2.6.31-rc5) – amd64 (x86_64):



Unusual bugs

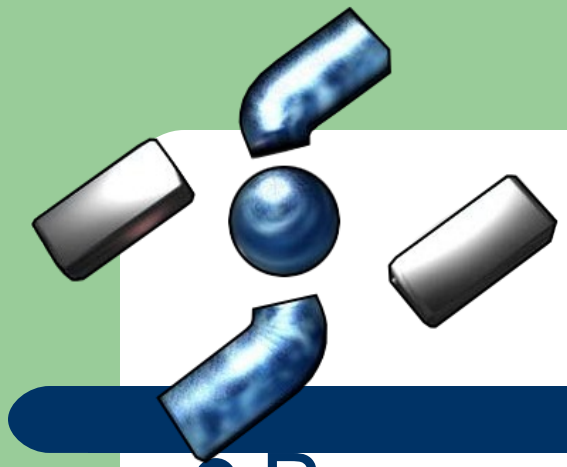
- Bugs:
  - [glibc] fenomen funkcji dn_expand():



Unusual bugs

- Bugs:
  - [glibc] fenomen funkcji dn_expand():

```
int dn_expand(unsigned char *msg, unsigned char *eomorig,
        unsigned char *comp_dn, unsigned char *exp_dn,
        int length);
```

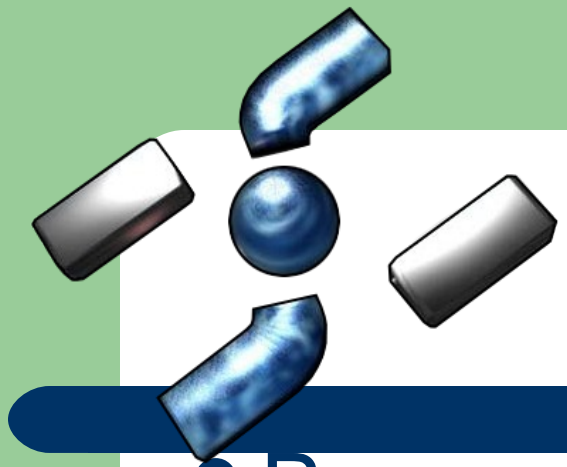


Unusual bugs

- Bugs:
  - [glibc] fenomen funkcji dn_expand():

```
int dn_expand(unsigned char *msg, unsigned char *eomorig,
              unsigned char *comp_dn, unsigned char *exp_dn,
              int length);
```

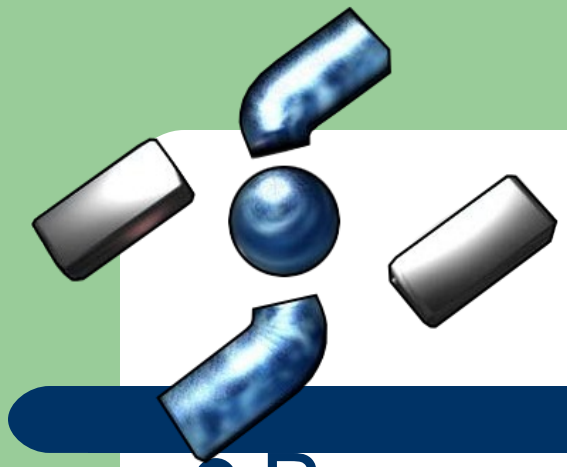
„Funkcja ta rozwija skompresowane nazwy domen 'comp_dn' do pełnych nazw domen, które są umieszczane w buforze 'exp_dn'o rozmiarze 'length'.”



Unusual bugs

- Bugs:
  - [glibc] fenomen funkcji dn_expand():

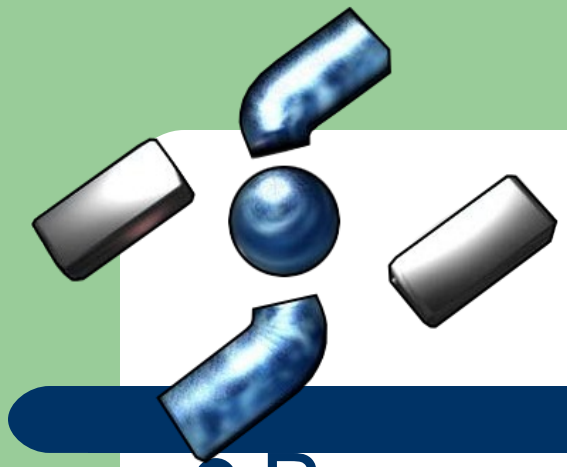
```
"resolv/res_comp.c"
Int dn_expand(const u_char *msg, const u_char *eom, const u_char *src,
        char *dst, int dstsiz) {
      int n = ns_name_uncompress(msg, eom, src, dst, (size_t)dstsiz);
      if (n > 0 && dst[0] == '.')
            dst[0] = '\0';
      return (n);
}
libresolv_hidden_def (dn_expand)
```



Unusual bugs

- Bugs:
  - [glibc] fenomen funkcji dn_expand():

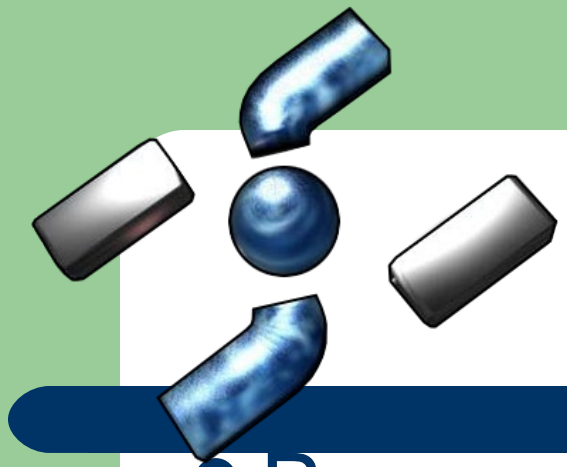
```
"resolv/res_comp.c"
Int dn_expand(const u_char *msg, const u_char *eom, const u_char *src,
        char *dst, int dstsiz) {
      int n = ns_name_uncompress(msg, eom, src, dst, (size_t)dstsiz);
      if (n > 0 && dst[0] == '.')
            dst[0] = '\0';
      return (n);
}
libresolv_hidden_def (dn_expand)
```



Unusual bugs

- Bugs:
  - [glibc] fenomen funkcji dn_expand():

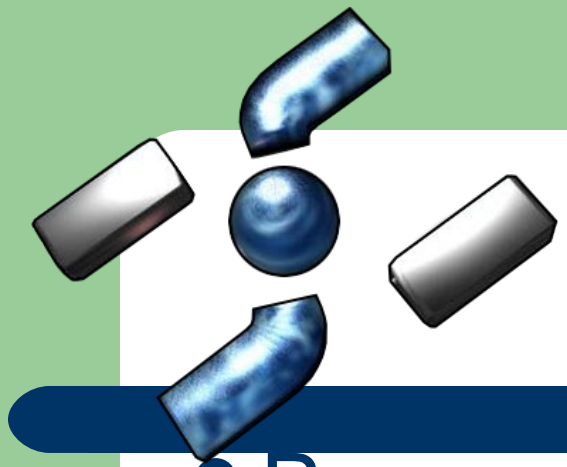
```
"resolv/ns_name.c"
Int ns_name_uncompress(const u_char *msg, const u_char *eom, const u_char *src,
                char *dst, size_t dstsiz) {
        u_char tmp[NS_MAXCDNAME];
        int n;
        ...
        if (ns_name_ntop(tmp, dst, dstsiz) == -1)
                return (-1);
        return (n);
}
```



Unusual bugs

- Bugs:
  - [glibc] fenomen funkcji dn_expand():

```
"resolv/ns_name.c"
Int ns_name_uncompress(const u_char *msg, const u_char *eom, const u_char *src,
                char *dst, size_t dstsiz) {
        u_char tmp[NS_MAXCDNAME];
        int n;
        ...
        if (ns_name_ntop(tmp, dst, dstsiz) == -1)
                return (-1);
        return (n);
}
```



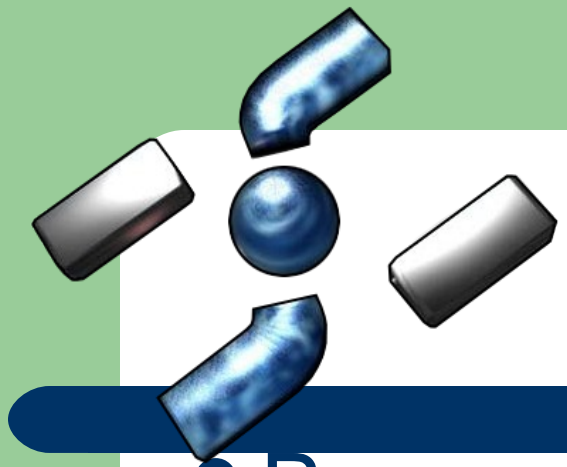
Unusual bugs

- Bugs:
  - [glibc] fenomen funkcji dn_expand():

"resolv/ns_name.c"

```
int ns_name_ntop(const u_char *src, char *dst, size_t dstsiz) {
...
        while ((n = *cp++) != 0) {
            ...
                if (n == 0x41) {
                    ...
                      *dn++ = '\\';
                      *dn++ = '[';
                      *dn++ = 'x';
```

<hexdump stringa>



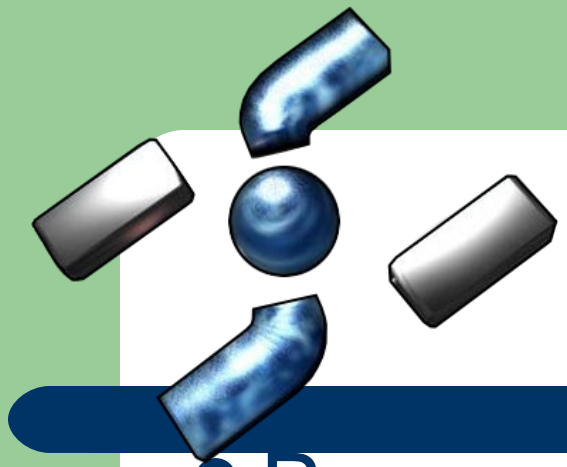
Unusual bugs

- Bugs:
  - [glibc] fenomen funkcji dn_expand():

"resolv/ns_name.c"

```
int ns_name_ntop(const u_char *src, char *dst, size_t dstsiz) {
...
        while ((n = *cp++) != 0) {
          ...
            if (n == 0x41) {
                ...
                  *dn++ = '\\';
                  *dn++ = '[';
                  *dn++ = 'x';
```

<hexdump stringa>



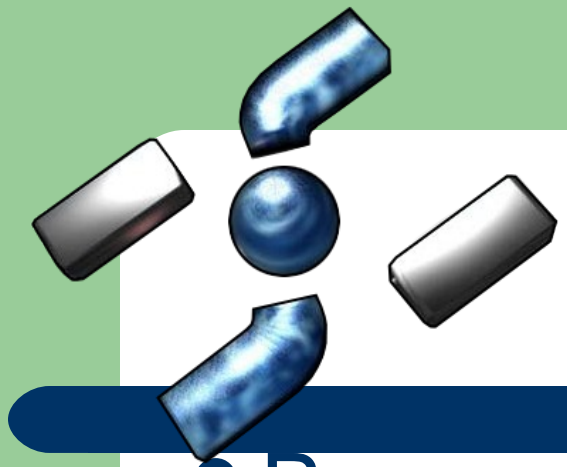
Unusual bugs

- Bugs:
  - [glibc] fenomen funkcji dn_expand():

"resolv/ns_name.c"

```
int ns_name_ntop(const u_char *src, char *dst, size_t dstsiz) {
...
        while ((n = *cp++) != 0) {
          ...
              if (n == 0x41) {
                  ...
                    *dn++ = '\\';
                    *dn++ = '[';
                    *dn++ = 'x';
```

<hexdump stringa>



Unusual bugs

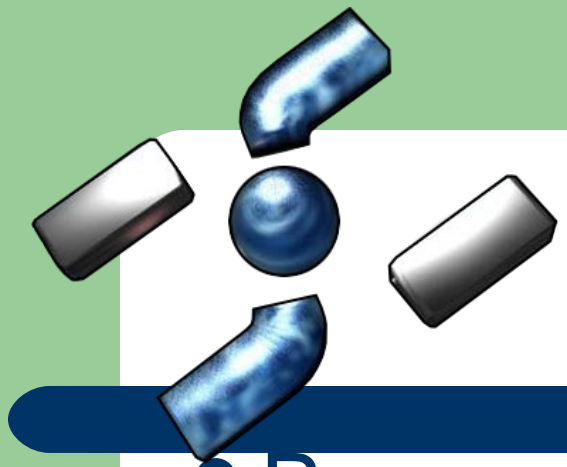
- Bugs:

Max domain_length == 256 => ~(256*4) = 1024.

Unusual bugs

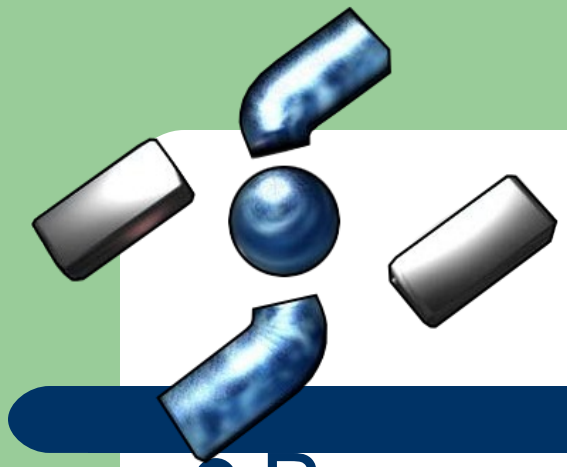
- Bugs:

Max domain_length == 256 => ~(256*4) = 1024.



Unusual bugs

- Bugs:
  - dn_expand() - real world – mtr (<= 0.72):



Unusual bugs

- Bugs:
  - dn_expand() - real world – mtr (<= 0.72):

"split.c"

```
#define MAX_LINE_SIZE 256
void split_redraw(void) {
  ...
  char newLine[MAX_LINE_SIZE];
  ...
     name = dns_lookup(addr);                    [1]
     if(name != NULL) {
       /* May be we should test name's length */      [!!]
       sprintf(newLine, "%s %d %d %d %d %d %d", name,    [2]
  ...
```

Unusual bugs

- Bugs:
  - dn_expand() - real world – mtr (<= 0.72):

"split.c"

```
#define MAX_LINE_SIZE 256
void split_redraw(void) {
  ...
  char newLine[MAX_LINE_SIZE];
  ...
     name = dns_lookup(addr);                    [1]
     if(name != NULL) {
       /* May be we should test name's length */      [!!]
       sprintf(newLine, "%s %d %d %d %d %d %d", name,    [2]
  ...
```

Unusual bugs

- Bugs:
  - dn_expand() - real world – mtr (<= 0.72):

"split.c"

```
#define MAX_LINE_SIZE 256
void split_redraw(void) {
  ...
  char newLine[MAX_LINE_SIZE];
  ...
     name = dns_lookup(addr);                    [1]
     if(name != NULL) {
       /* May be we should test name's length */      [!!]
       sprintf(newLine, "%s %d %d %d %d %d %d", name,    [2]
  ...
```

Unusual bugs

- Bugs:
  - dn_expand() - real world – mtr (<= 0.72):

"dns.c"

```
void parserespacket(byte *s, int l) {
  ...
        r = dn_expand(s,s + l,c,namestring,MAXDNAME);
   ...
}
```

Unusual bugs

- Bugs:
  - dn_expand() - real world – mtr (<= 0.72):

"dns.c"

```
void parserespacket(byte *s, int l) {
  ...
        r = dn_expand(s,s + l,c,namestring,MAXDNAME);
   ...
}
```

"dns.c"

```
char namestring[1024+1];
```

Unusual bugs

- Bugs:
  - dn_expand() - real world – mtr (<= 0.72):

"dns.c"

```
void parserespacket(byte *s, int l) {
  ...
        r = dn_expand(s,s + l,c,namestring,MAXDNAME);
   ...
}
```

"dns.c"

```
char namestring[1024+1];
```

"/usr/include/arpa/nameser.h"

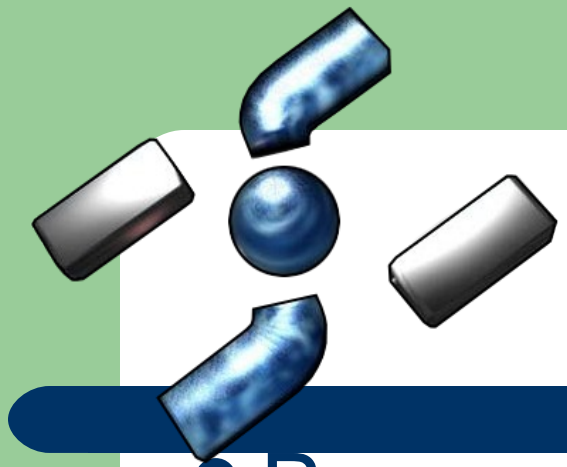
```
#define NS_MAXDNAME 1025 /* maximum domain name */
```

Unusual bugs

- Bugs:
  - dn_expand() - real world – mtr (<= 0.72):

Unusual bugs

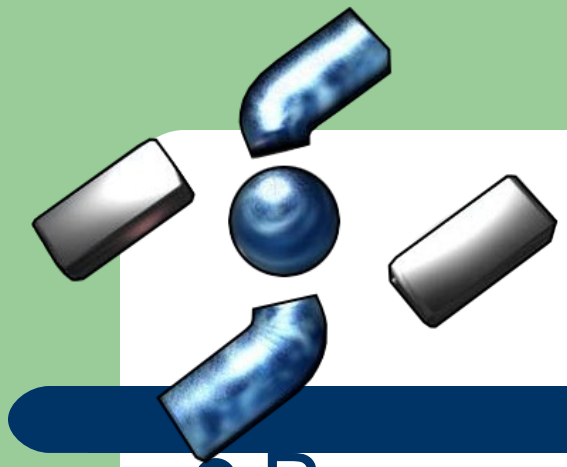
- Bugs:
  - Pointer check vulnerability:



Unusual bugs

- Bugs:
  - Pointer check vulnerability:

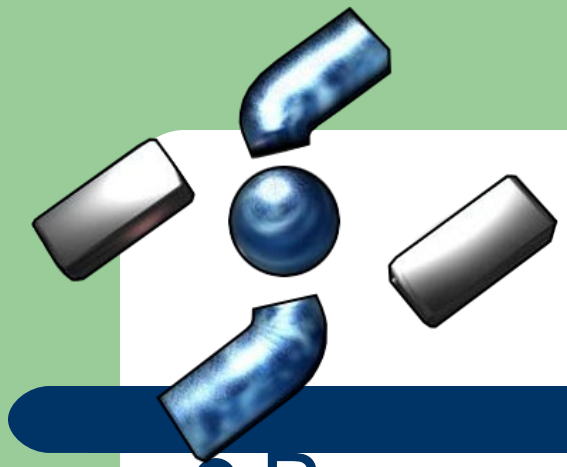
```
int main(int argc, char *argv[]) {
   char *ptr;
   if (argc != 2)
      exit(-1);
   ptr = (char *)strtoll(argv[1],NULL,10);
   memcpy(ptr,"pi3 was here ;-)",strlen("pi3 was here ;-)"));
   printf("%s\n",ptr);
   return 0;
}
```



Unusual bugs

- Bugs:
  - Pointer check vulnerability:

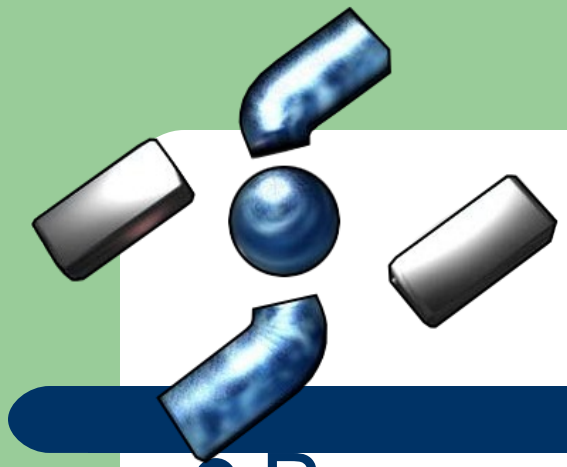
```
int main(int argc, char *argv[]) {
   char *ptr;
   if (argc != 2)
      exit(-1);
   ptr = (char *)strtoll(argv[1],NULL,10);
   memcpy(ptr,"pi3 was here ;-)",strlen("pi3 was here ;-)"));
   printf("%s\n",ptr);
   return 0;
}
```



Unusual bugs

- Bugs:
  - Pointer check vulnerability:

```
int main(int argc, char *argv[]) {
   char *ptr;
   if (argc != 2)
      exit(-1);
   ptr = (char *)strtoll(argv[1],NULL,10);
   memcpy(ptr,"pi3 was here ;-)",strlen("pi3 was here ;-)"));
   printf("%s\n",ptr);
   return 0;
}
```



Unusual bugs

- Bugs:
  - Pointer check vulnerability:

```
int main(int argc, char *argv[]) {
   char *ptr;
   if (argc != 2)
      exit(-1);
   ptr = (char *)strtoll(argv[1],NULL,10);
   memcpy(ptr,"pi3 was here ;-)",strlen("pi3 was here ;-)"));
   printf("%s\n",ptr);
   return 0;
}
```

Unusual bugs

- Bugs:
  - Pointer check vulnerability:

(gdb) r 2

Starting program: /media/truecrypt1/Prezentacje/Secday/2 2

Program received signal SIGSEGV, Segmentation fault.

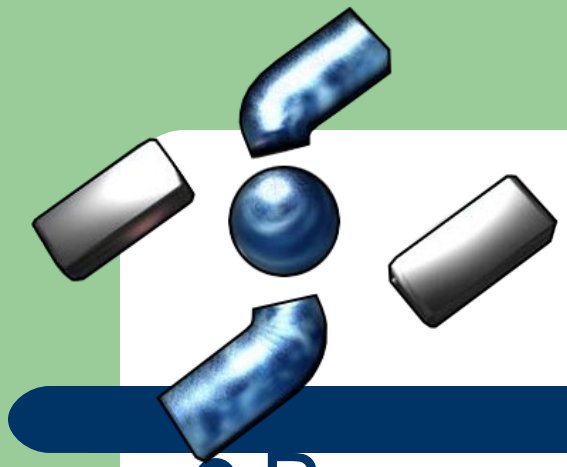
0x00b50651 in memcpy () from /lib/libc.so.6

Missing separate debuginfos, use: debuginfo-install glibc-2.9-3.i686

(gdb) bt

#0 0x00b50651 in memcpy () from /lib/libc.so.6

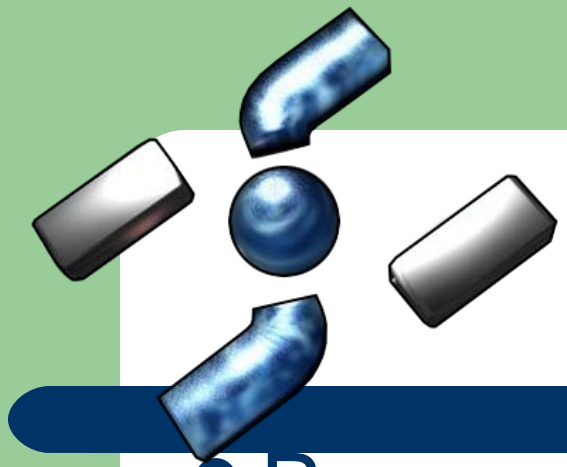
#1 0x080484bd in main ()



Unusual bugs

- Bugs:
  - Pointer check vulnerability:

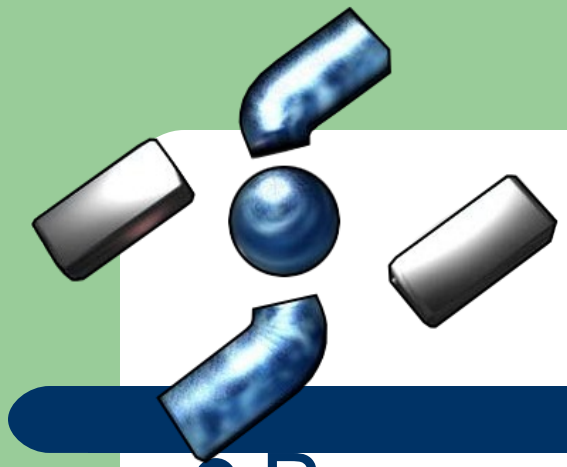
```
(gdb) x/i $eip
0xb50651 <memcpy+97>:    rep movsl %ds:(%esi),%es:(%edi)
(gdb) i r esi edi
esi            0x80485a4    134514084
edi            0x2       2
(gdb) p/d 0xbfffee01
$1 = 3221220865
(gdb) r 3221220865
...
pi3 was here ;-)p
Program exited normally.
```



Unusual bugs

- Bugs:
  - Pointer check vulnerability:

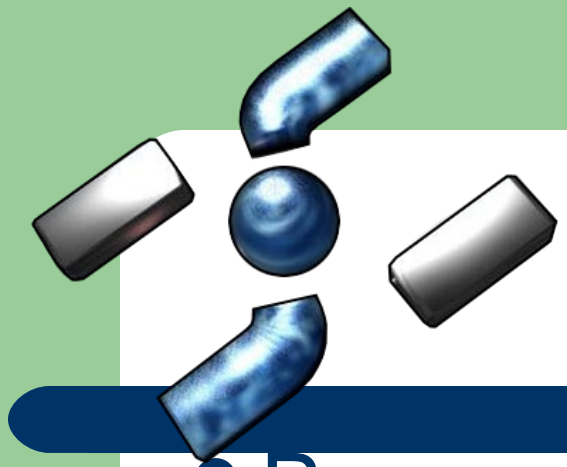
```
(gdb) x/i $eip
0xb50651 <memcpy+97>:    rep movsl %ds:(%esi),%es:(%edi)
(gdb) i r esi edi
esi            0x80485a4    134514084
edi            0x2          2
(gdb) p/d 0xbfffee01
$1 = 3221220865
(gdb) r 3221220865
...
pi3 was here ;-)p
Program exited normally.
```



Unusual bugs

- Bugs:
  - Pointer check vulnerability:

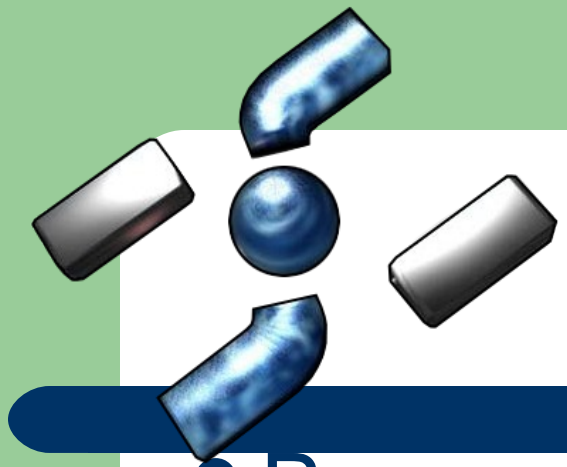
```
(gdb) x/i $eip
0xb50651 <memcpy+97>:    rep movsl %ds:(%esi),%es:(%edi)
(gdb) i r esi edi
esi            0x80485a4    134514084
edi            0x2      2
(gdb) p/d 0xbfffee01
$1 = 3221220865
(gdb) r 3221220865
...
pi3 was here ;-)p
Program exited normally.
```



Unusual bugs

- Bugs:
  - Pointer check vulnerability:

```
(gdb) x/i $eip
0xb50651 <memcpy+97>:    rep movsl %ds:(%esi),%es:(%edi)
(gdb) i r esi edi
esi            0x80485a4    134514084
edi            0x2      2
(gdb) p/d 0xbfffee01
$1 = 3221220865
(gdb) r 3221220865
...
pi3 was here ;-)p
Program exited normally.
```



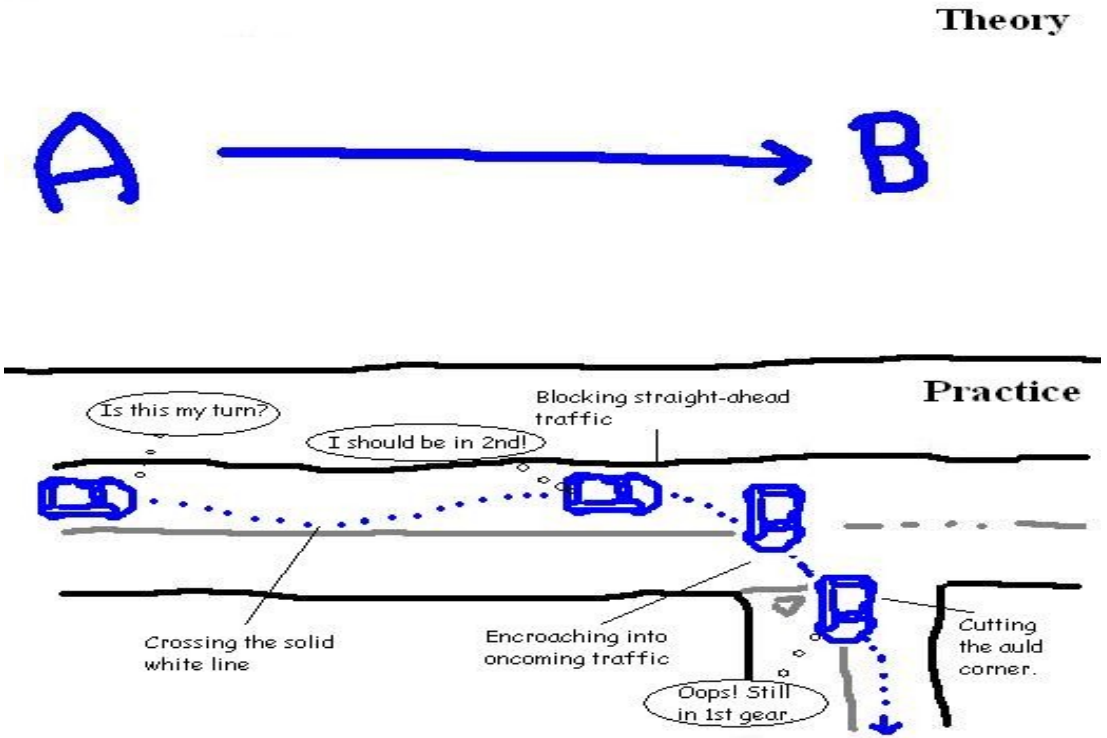
Unusual bugs

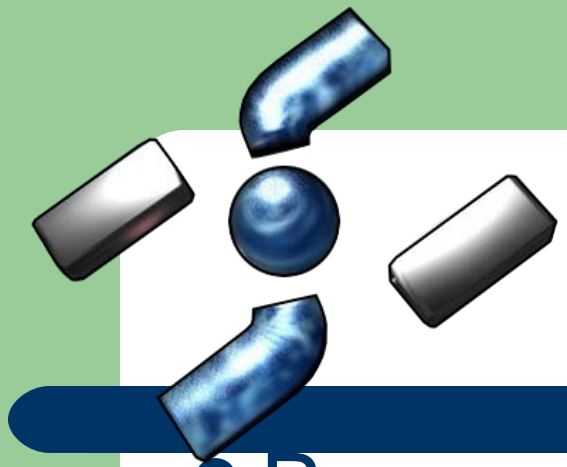
- Bugs:
  - Pointer check vulnerability:

```
(gdb) x/i $eip
0xb50651 <memcpy+97>:    rep movsl %ds:(%esi),%es:(%edi)
(gdb) i r esi edi
esi            0x80485a4    134514084
edi            0x2      2
(gdb) p/d 0xbfffee01
$1 = 3221220865
(gdb) r 3221220865
...
pi3 was here ;-)p
Program exited normally.
```

Unusual bugs

- Bugs:
  - Pointer check vulnerability – real world:

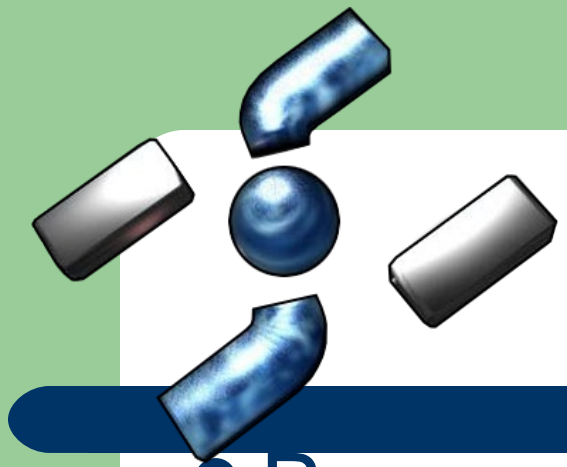




Unusual bugs

- Bugs:
  - Pointer check vulnerability – real world:

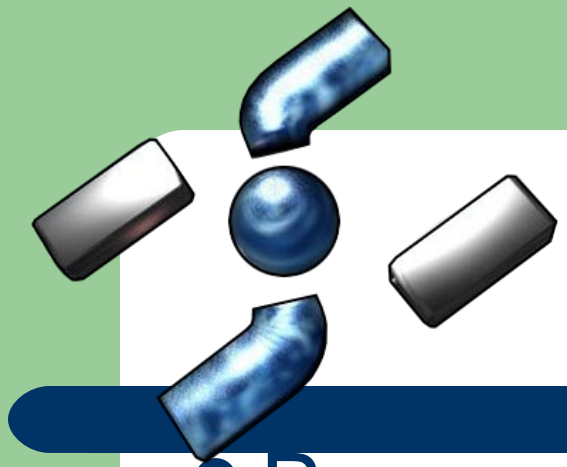
Linux kernel vmsplice() vulnerability !!! :)



Unusual bugs

- Bugs:
  - Pointer check vulnerability – real world:

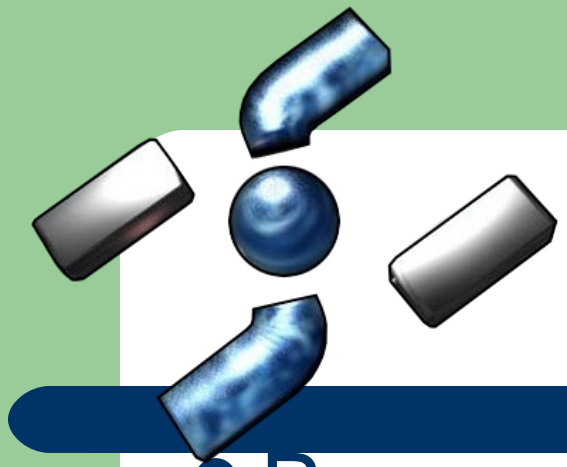
```
static long vmsplice_to_user(struct file *file, const struct iovec __user *iov,
                             unsigned long nr_segs, unsigned int flags)  {
        ...
          error = get_user(base, &iov->iov_base);
          if (unlikely(error))
                  break;
          error = get_user(len, &iov->iov_len);
          if (unlikely(error))
                  break;
        ...
```



Unusual bugs

- Bugs:
  - Pointer check vulnerability – real world:

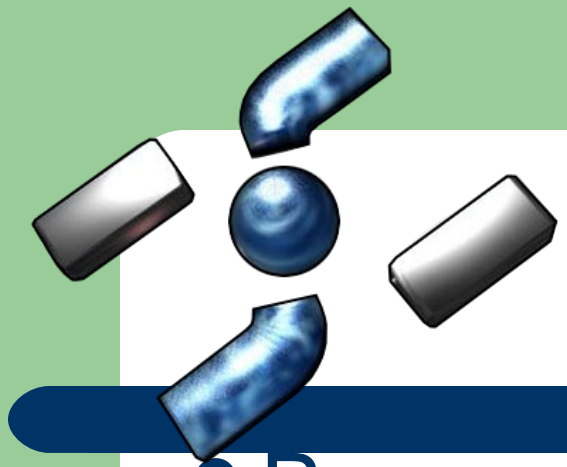
```
static long vmsplice_to_user(struct file *file, const struct iovec __user *iov,
                             unsigned long nr_segs, unsigned int flags)  {
    ...
      error = get_user(base, &iov->iov_base);
      if (unlikely(error))
            break;
      error = get_user(len, &iov->iov_len);
      if (unlikely(error))
            break;
    ...
```



Unusual bugs

- Bugs:
  - Pointer check vulnerability – real world:

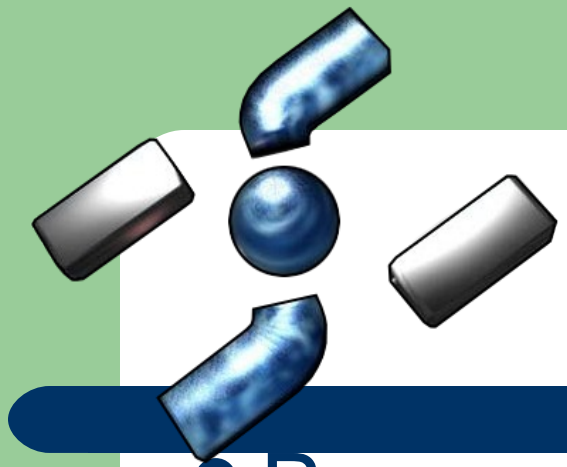
```
...
        if (unlikely(!len))
                break;
        if (unlikely(!base)) {
                error = -EFAULT;
                break;
        }
...
```



Unusual bugs

- Bugs:
  - Pointer check vulnerability – real world:

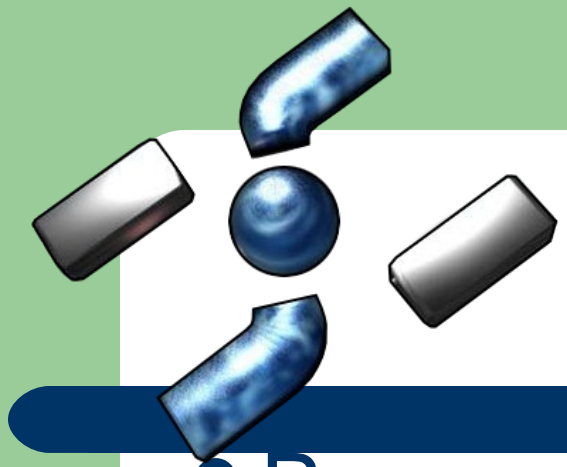
```
...
        sd.len = 0;
        sd.total_len = len;
        sd.flags = flags;
        sd.u.userptr = base;
        sd.pos = 0;

        size = __splice_from_pipe(pipe, &sd, pipe_to_user);
...
```



Unusual bugs

- Bugs:
  - Pointer check vulnerability – real world:

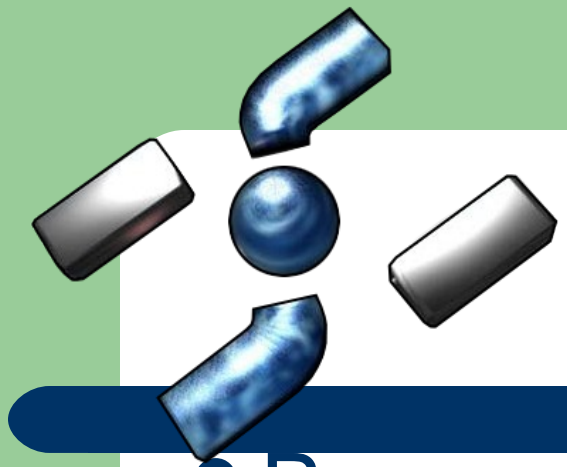
```
...
        sd.len = 0;
        sd.total_len = len;
        sd.flags = flags;
        sd.u.userptr = base;
        sd.pos = 0;

        size = __splice_from_pipe(pipe, &sd, pipe_to_user);
...
```



Unusual bugs

- Bugs:
  - Pointer check vulnerability – real world:

```
...
        sd.len = 0;
        sd.total_len = len;
        sd.flags = flags;
        sd.u.userptr = base;
        sd.pos = 0;

        size = __splice_from_pipe(pipe, &sd, pipe_to_user);
...
```



Unusual bugs

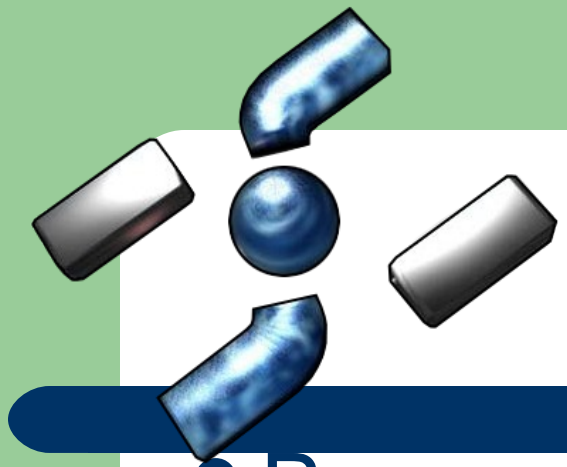
- Bugs:
  - Pointer check vulnerability – real world:

```
...
        sd.len = 0;
        sd.total_len = len;
        sd.flags = flags;
        sd.u.userptr = base;
        sd.pos = 0;

        size = __splice_from_pipe(pipe, &sd, pipe_to_user);
...
```

Unusual bugs

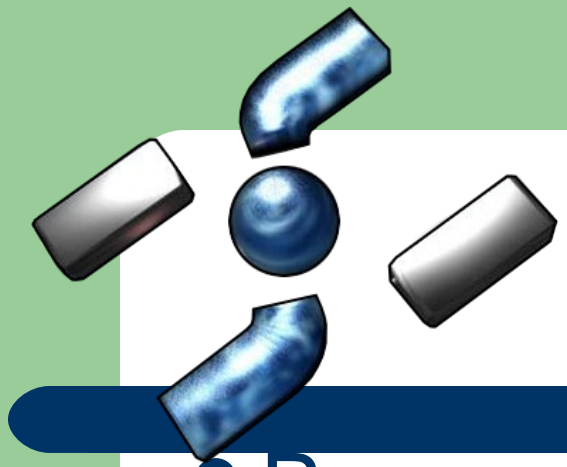
- Bugs:
  - Pointer check vulnerability – real world:

Smile



Unusual bugs

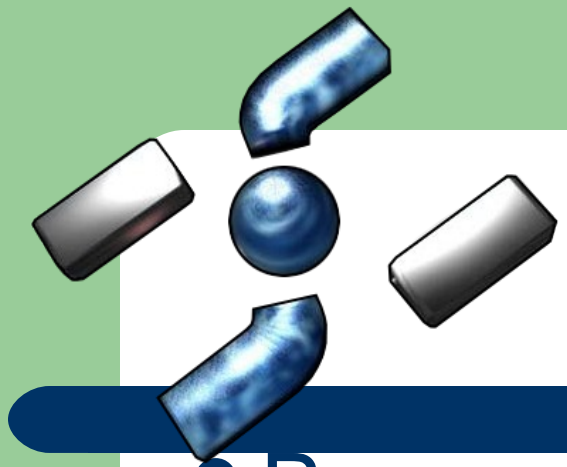
- Bugs:
  - Gcc optimalization – real world:



Unusual bugs

- Bugs:
  - Gcc optimalization – real world:

Linux kernel (2.6.30 && 2.6.31) /dev/net/tun NULL pointer Dereference

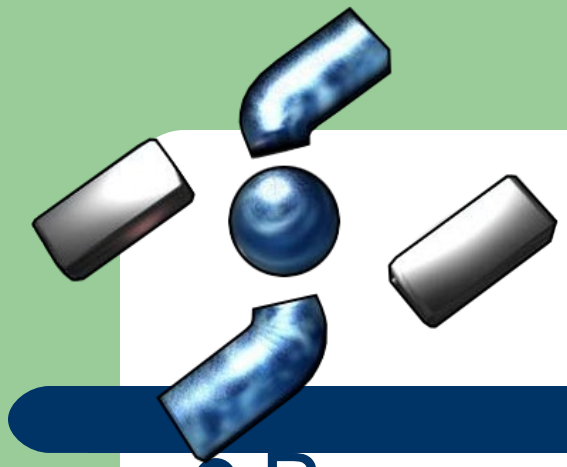


Unusual bugs

- Bugs:
  - Gcc optimalization – real world:

Linux kernel (2.6.30 && 2.6.31) /dev/net/tun NULL pointer Dereference

Dzieki optymalizacji w gcc – exploitowalny błąd :)

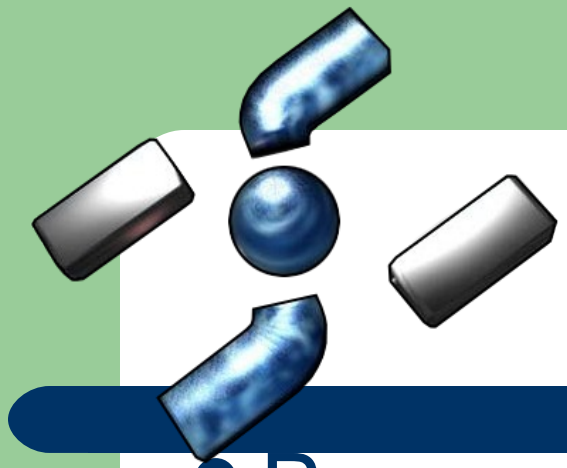


Unusual bugs

- Bugs:
  - Gcc optimalization – real world:

"drivers/net/tun.c"

```
static unsigned int tun_chr_poll(struct file *file, poll_table * wait)
{
        struct tun_file *tfile = file->private_data;
        struct tun_struct *tun = __tun_get(tfile);
        struct sock *sk = tun->sk;
        unsigned int mask = 0;
        if (!tun)
                return POLLERR;
    ...
```

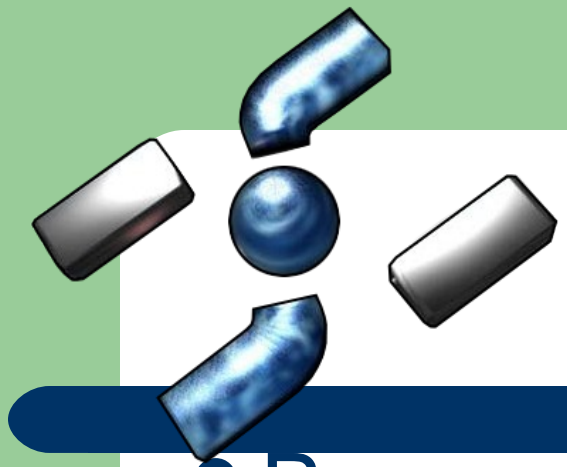


Unusual bugs

- Bugs:
  - Gcc optimalization – real world:

"drivers/net/tun.c"

```
static unsigned int tun_chr_poll(struct file *file, poll_table * wait)
{
        struct tun_file *tfile = file->private_data;
        struct tun_struct *tun = __tun_get(tfile);
        struct sock *sk = tun->sk;
        unsigned int mask = 0;
        if (!tun)
                return POLLERR;
    ...
```

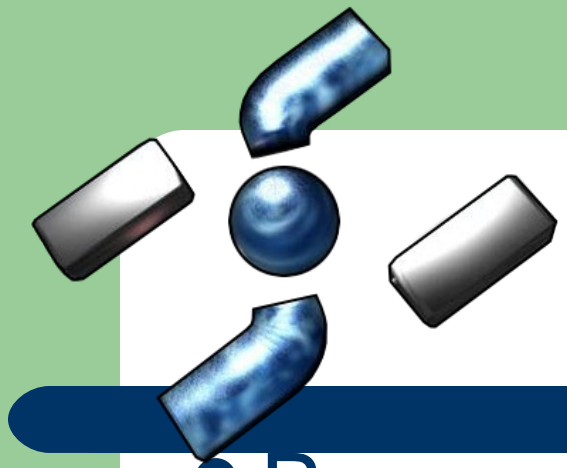


Unusual bugs

- Bugs:
  - Gcc optimalization – real world:

"drivers/net/tun.c"

```
static unsigned int tun_chr_poll(struct file *file, poll_table * wait)
{
        struct tun_file *tfile = file->private_data;
        struct tun_struct *tun = __tun_get(tfile);
        struct sock *sk = tun->sk;
        unsigned int mask = 0;
        if (!tun)
                return POLLERR;
    ...
```

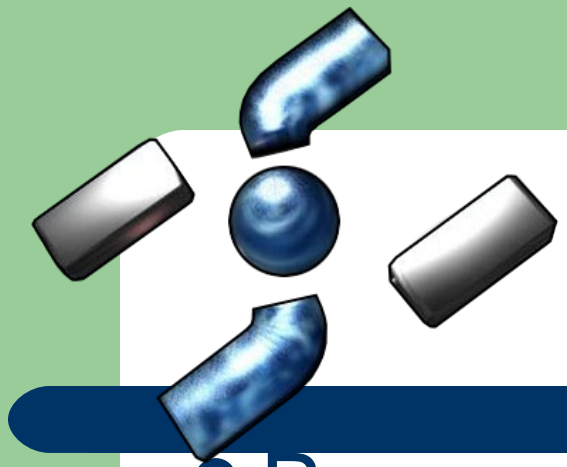


Unusual bugs

- Bugs:
  - Gcc optimalization – real world:

"drivers/net/tun.c"

```
static unsigned int tun_chr_poll(struct file *file, poll_table * wait)
{
        struct tun_file *tfile = file->private_data;
        struct tun_struct *tun = __tun_get(tfile);
        struct sock *sk = tun->sk;
        unsigned int mask = 0;
        if (!tun)
                return POLLERR;
    ...
```



Unusual bugs

- Bugs:
  - Gcc optimalization – real world:

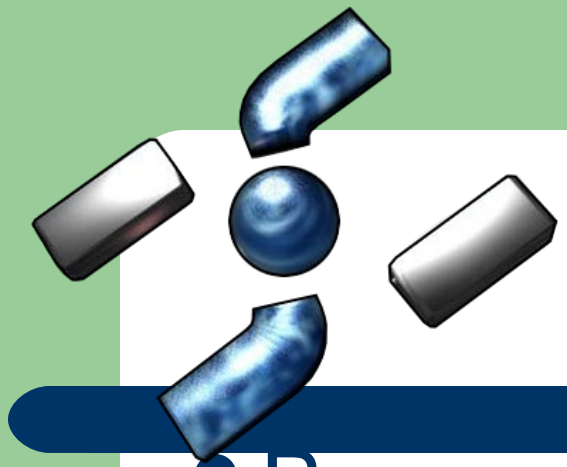
"drivers/net/tun.c"

```
static unsigned int tun_chr_poll(struct file *file, poll_table * wait)
{
        struct tun_file *tfile = file->private_data;
        struct tun_struct *tun = __tun_get(tfile);
        struct sock *sk = tun->sk;
        unsigned int mask = 0;
        if (!tun)
                return POLLERR;
    ...
```

Unusual bugs

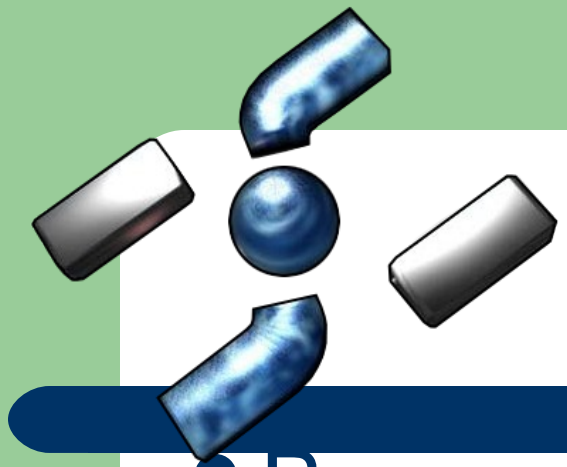
- Bugs:
  - Gcc optimalization – real world:

Smile



Unusual bugs

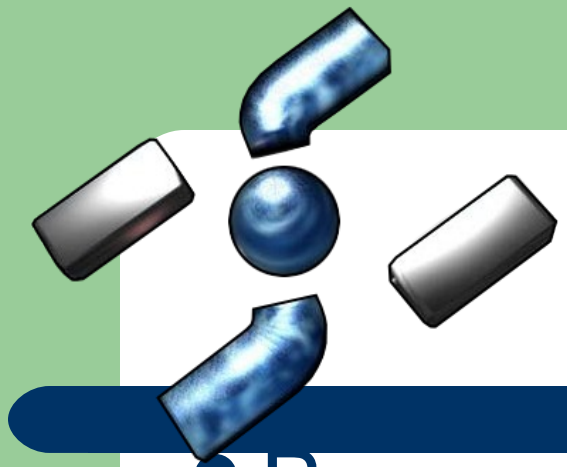
- Bugs:
  - Logic compare registers bug – real world:



Unusual bugs

- Bugs:
  - Logic compare registers bug – real world:

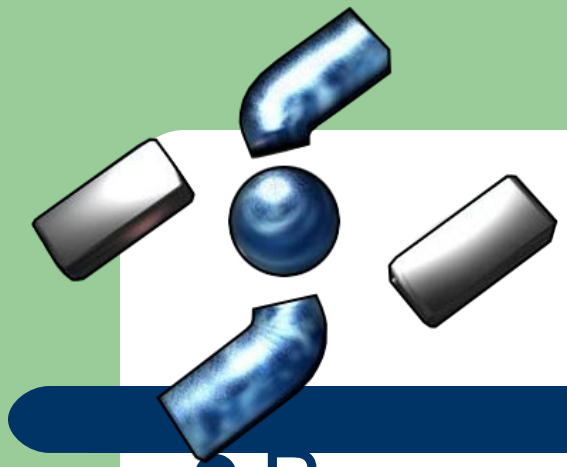
Linux kernel IA32 System Call Emulation Vulnerability



Unusual bugs

- Bugs:
  - Logic compare registers bug – real world:

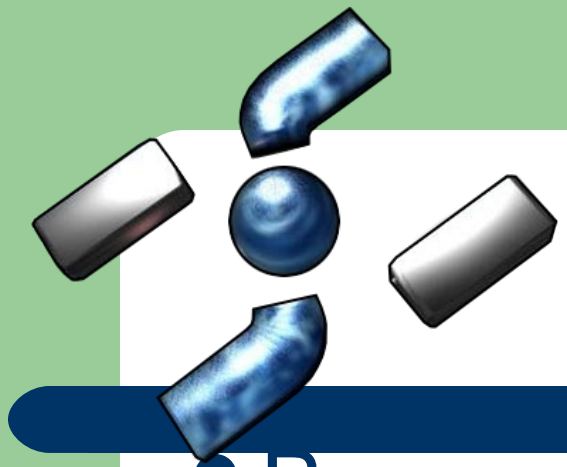
```
sysenter_do_call:
        cmpl    $(IA32_NR_syscalls-1),%eax
        ja      ia32_badsys
        IA32_ARG_FIXUP 1
        call    *ia32_sys_call_table(,%rax,8)
```



Unusual bugs

- Bugs:
  - Logic compare registers bug – real world:

```
sysenter_do_call:
        cmpl    $(IA32_NR_syscalls-1),%eax
        ja      ia32_badsys
        IA32_ARG_FIXUP 1
        call    *ia32_sys_call_table(,%rax,8)
```



Unusual bugs

- Bugs:
  - Logic compare registers bug – real world:

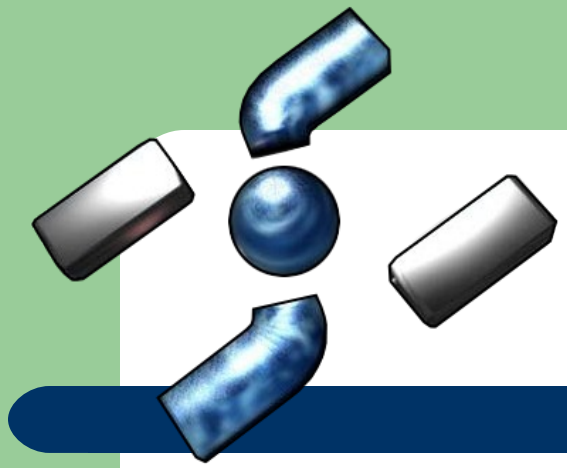
```
sysenter_do_call:
        cmpl    $(IA32_NR_syscalls-1),%eax
        ja      ia32_badsys
        IA32_ARG_FIXUP 1
        call    *ia32_sys_call_table(,%rax,8)
```

Unusual bugs

- Bugs:
  - Logic compare registers bug – real world:

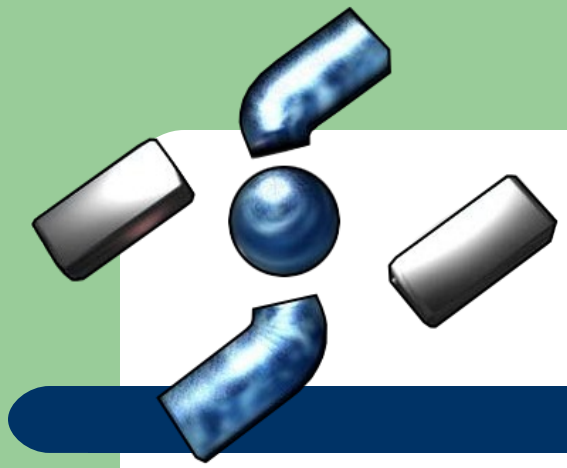
Unusual bugs

- Losowe przemyślenia:



Unusual bugs

- Losowe przemyślenia:
  - Pisanie do stderr :)

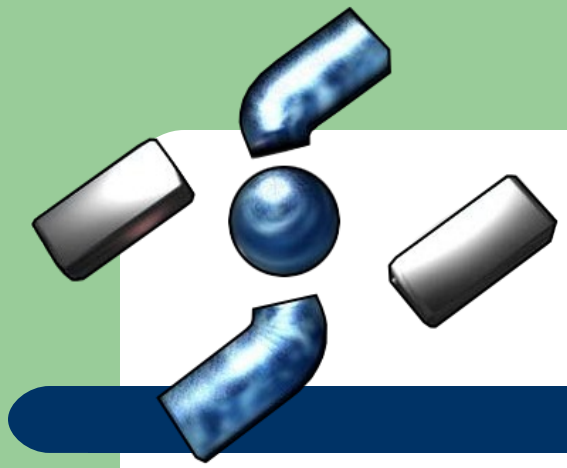


Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

- Losowe przemyślenia:
  - Pisanie do stderr :)
    - Aplikacja zamyka deskryptory (załóżmy stderr)

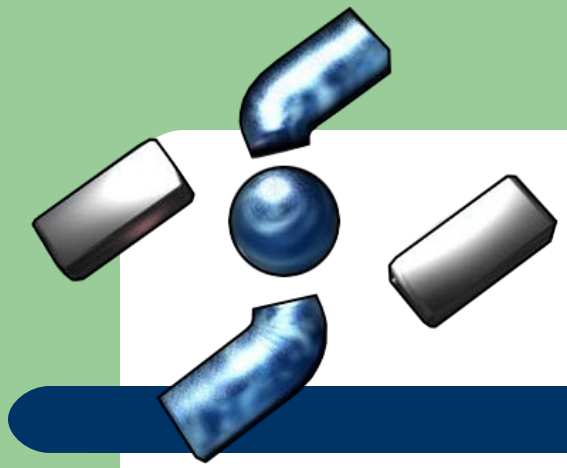


Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

- Losowe przemyślenia:
  - Pisanie do stderr :)
    - Aplikacja zamyka deskryptory (załóżmy stderr)
    - Aplikacja otwiera plik...

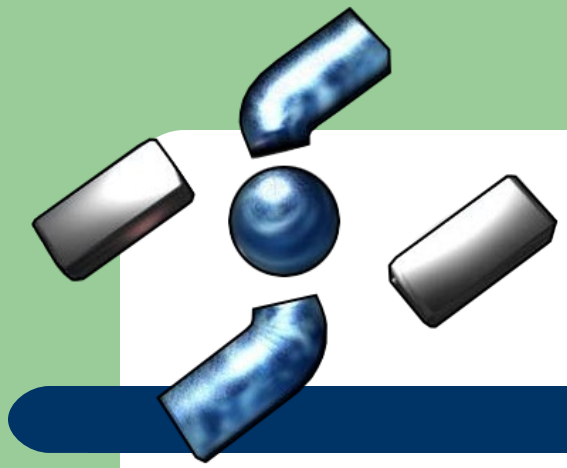


Hispasec Sistemas

Seguridad y Tecnologías de la Información

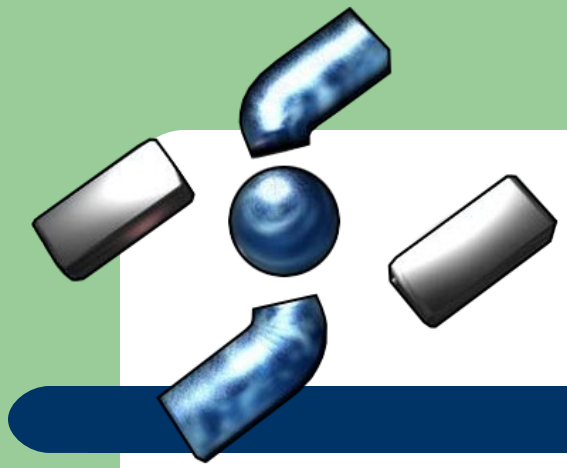
Unusual bugs

- Losowe przemyślenia:
  - Pisanie do stderr :)
    - Aplikacja zamyka deskryptory (załóżmy stderr)
    - Aplikacja otwiera plik...
    - Dostaję najniższy wolny deskryptor (2 - stderr)



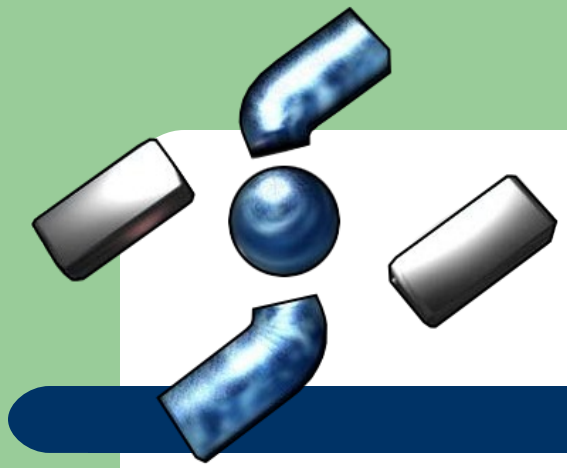
Unusual bugs

- Losowe przemyślenia:
  - Pisanie do stderr :)
    - Aplikacja zamyka deskryptory (załóżmy stderr)
    - Aplikacja otwiera plik...
    - Dostaję najniższy wolny deskryptor (2 – stderr)
    - Wymuszamy błąd aplikacyjny - jakikolwiek



Unusual bugs

- Losowe przemyślenia:
  - Pisanie do stderr :)
    - Aplikacja zamyka deskryptory (załóżmy stderr)
    - Aplikacja otwiera plik...
    - Dostaję najniższy wolny deskryptor (2 – stderr)
    - Wymuszamy błąd aplikacyjny – jakikolwiek
    - Raport o błędnym działaniu (np malloc()) wypisywany jest zazwyczaj na stderr

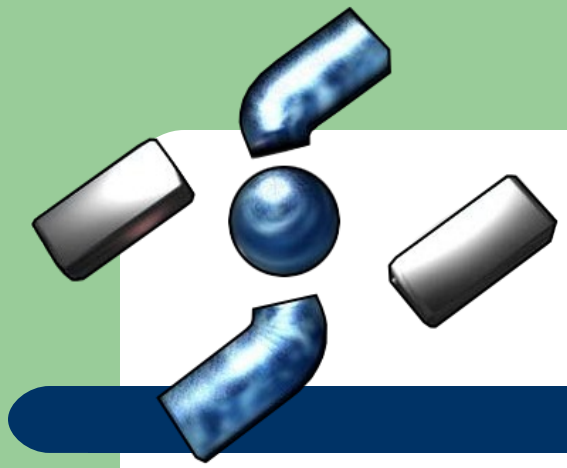


Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

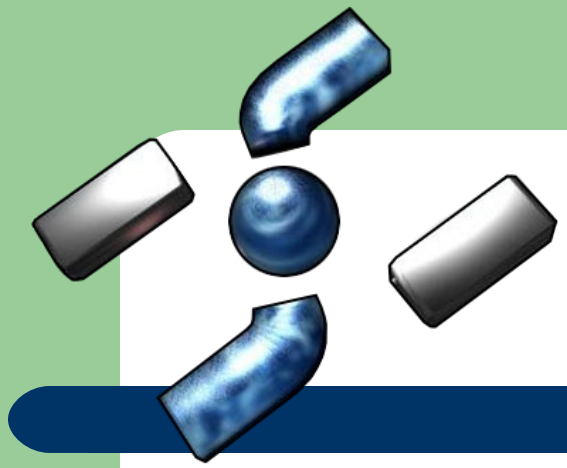
- Losowe przemyślenia:
  - Pisanie do stderr :)
    - Aplikacja zamyka deskryptory (załóżmy stderr)
    - Aplikacja otwiera plik...
    - Dostaję najniższy wolny deskryptor (2 – stderr)
    - Wymuszamy błąd aplikacyjny – jakikolwiek
    - Raport o błędnym działaniu (np malloc()) wypisywany jest zazwyczaj na stderr
    - Jeżeli zmusimy do otworzenia krytycznych plików systemowych mamy poważne zagrożenie (/etc/passwd?)



Unusual bugs

- Losowe przemyślenia – procmail:

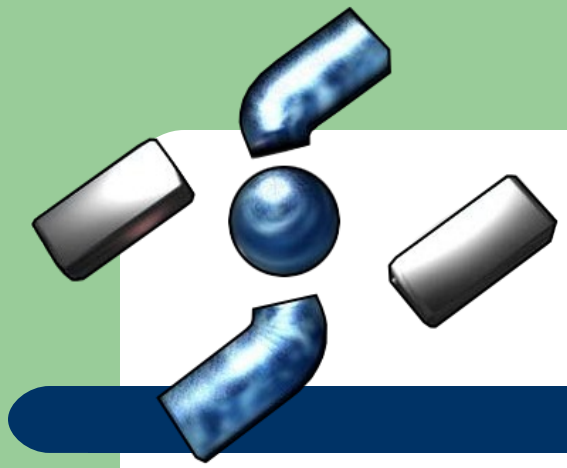
```
void*app_val_(sp,size)
struct dyna_array*const sp;
int size;
{
        if(sp->filled==sp->tspace) /* need to grow ? */
    {
      size_tlen=(sp->tspace+=4)*size;
        sp->vals=sp->vals?realloc(sp->vals,len):malloc(len);
    }
    return &sp->vals[size*sp->filled++];
}
```



Unusual bugs

- Losowe przemyślenia – procmail:

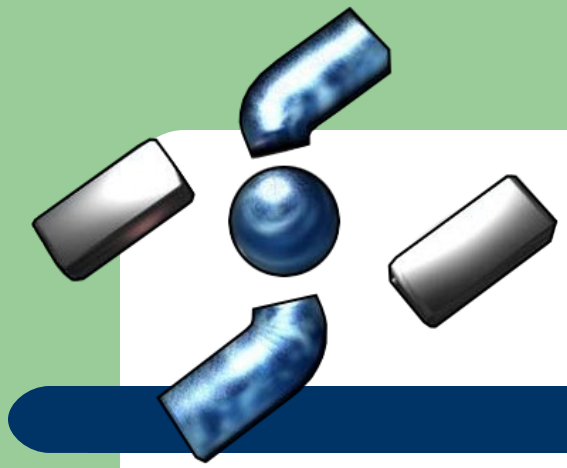
```
void*app_val_(sp,size)
struct dyna_array*const sp;
int size;
{
        if(sp->filled==sp->tspace) /* need to grow ? */
    {
      size_tlen=(sp->tspace+=4)*size;
        sp->vals=sp->vals?realloc(sp->vals,len):malloc(len);
    }
    return &sp->vals[size*sp->filled++];
}
```



Unusual bugs

- Losowe przemyślenia – procmail:

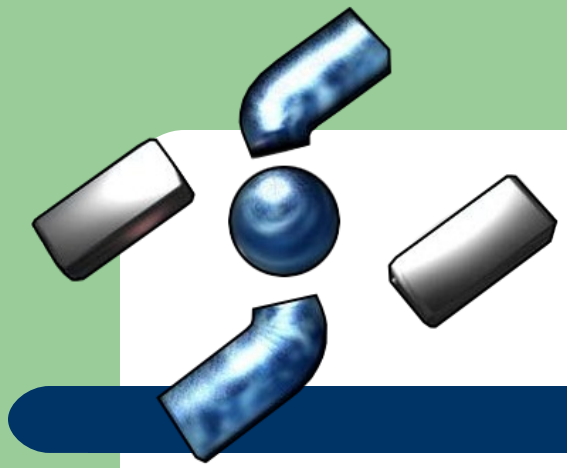
```
void*app_val_(sp,size)
struct dyna_array*const sp;
int size;
{
        if(sp->filled==sp->tspace) /* need to grow ? */
    {
      size_tlen=(sp->tspace+=4)*size;
        sp->vals=sp->vals?realloc(sp->vals,len):malloc(len);
    }
    return &sp->vals[size*sp->filled++];
}
```



Unusual bugs

- Losowe przemyślenia – theory:

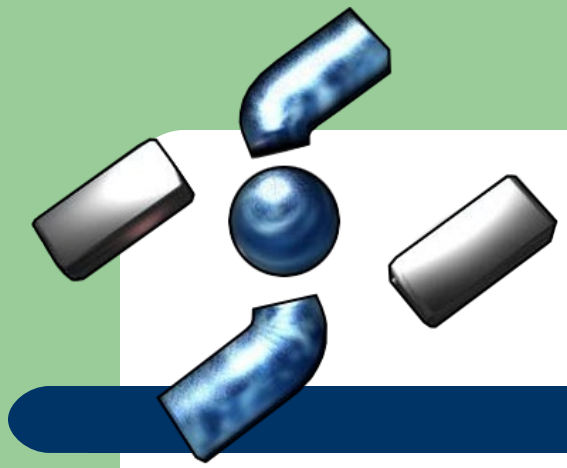
```
int main(int argc, char *argv[])  {

   char *ptr = NULL;

   if (argc != 2)
      exit(-1);

   ptr += strtoll(argv[1],NULL,10)
   memcpy(ptr,"pi3 was here ;-)",strlen("pi3 was here ;-)"));
   printf("%s\n",ptr);

}
```



Unusual bugs

- Losowe przemyślenia – theory:

```
int main(int argc, char *argv[])  {

   char *ptr = NULL;

   if (argc != 2)
      exit(-1);

   ptr += strtoll(argv[1],NULL,10)
   memcpy(ptr,"pi3 was here ;-)",strlen("pi3 was here ;-)"));
   printf("%s\n",ptr);

}
```



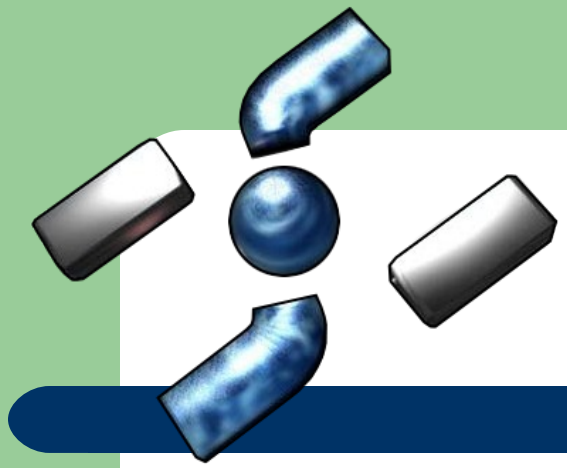
Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

- Losowe przemyślenia – theory:

```
int main(int argc, char *argv[])  {

   char *ptr = NULL;

   if (argc != 2)
      exit(-1);

   ptr += strtoll(argv[1],NULL,10)
   memcpy(ptr,"pi3 was here ;-)",strlen("pi3 was here ;-)"));
   printf("%s\n",ptr);

}
```



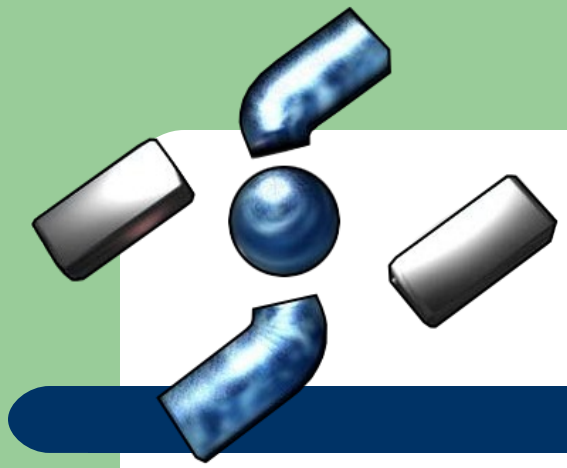
Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

- Losowe przemyślenia – theory:

```
int main(int argc, char *argv[])  {

   char *ptr = NULL;

   if (argc != 2)
      exit(-1);

   ptr += strtoll(argv[1],NULL,10)
   memcpy(ptr,"pi3 was here ;-)",strlen("pi3 was here ;-)"));
   printf("%s\n",ptr);

}
```



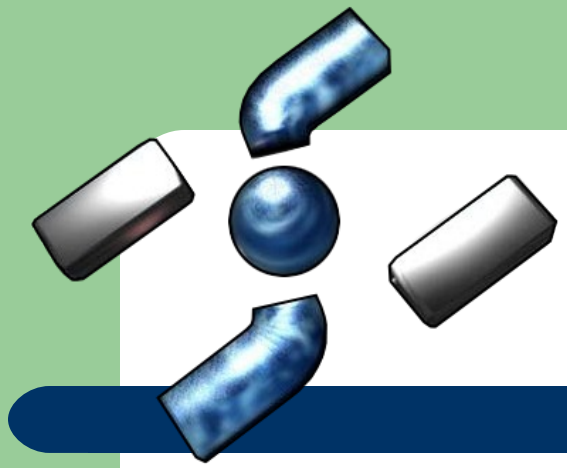
Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

- Losowe przemyślenia – theory:

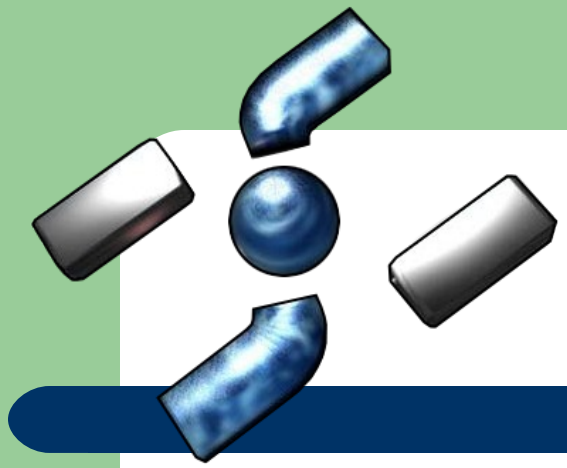
```
(gdb) r 2
Starting program: /media/truecrypt1/Prezentacje/Secday/3 2
Program received signal SIGSEGV, Segmentation fault.
0x00b50651 in memcpy () from /lib/libc.so.6
Missing separate debuginfos, use: debuginfo-install glibc-2.9-3.i686
(gdb) bt
#0  0x00b50651 in memcpy () from /lib/libc.so.6
#1  0x080484b4 in main ()
(gdb) i r
...
edi            0x2 2
...
```



Unusual bugs

- Losowe przemyślenia – theory:

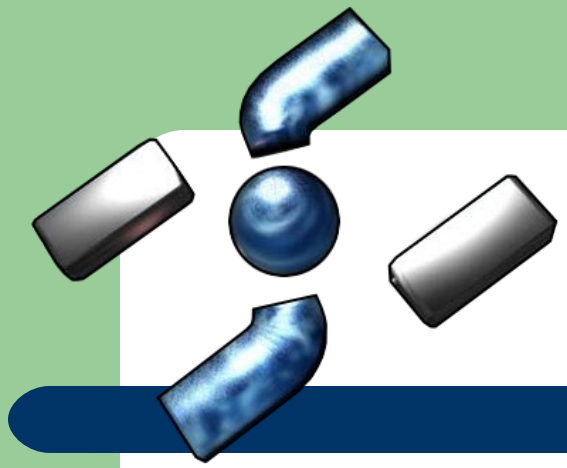
```
(gdb) x/i $eip
0xb50651 <memcpy+97>:      rep movsl %ds:(%esi),%es:(%edi)
(gdb) r 3221220865
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /media/truecrypt1/Prezentacje/Secday/3 3221220865
(no debugging symbols found)
(no debugging symbols found)
(no debugging symbols found)
pi3 was here ;-)p
Program exited with code 023.
(gdb)
```



Unusual bugs

- Losowe przemyślenia:

STACK EXHAUSTION



Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

?

Hispasec Sistemas

Seguridad y Tecnologías de la Información

Unusual bugs

DZIĘKUJĘ