



november **WEBBBBBBB**

`root@november ~ #`

Buffer Overflows

Arhitectura memoriei pentru x86

- Adresă logică (segmente)

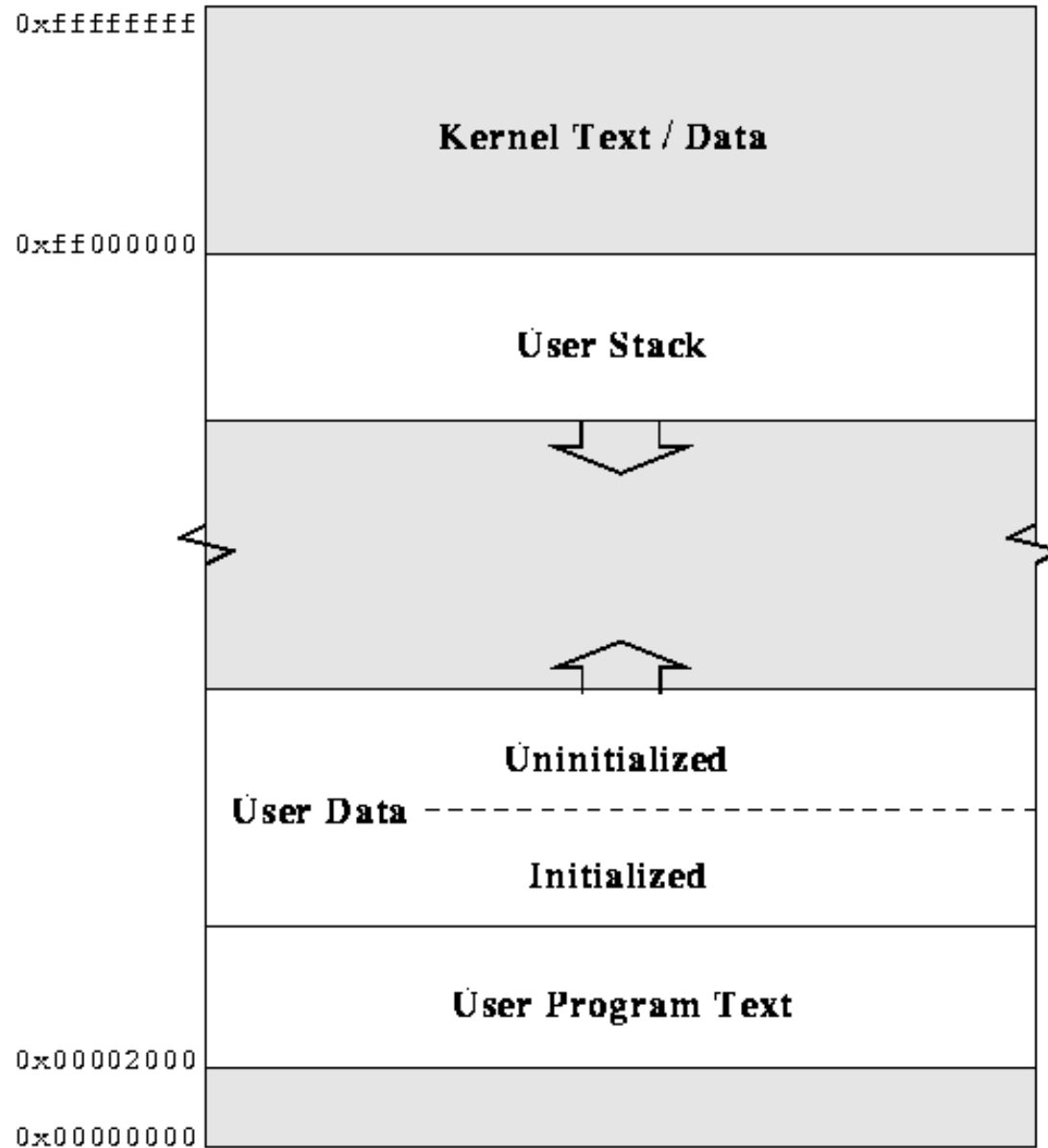
[segment:offset]

- Adresă lineară

0x00000000 – 0xffffffff (mașinile pe 32 de biți)

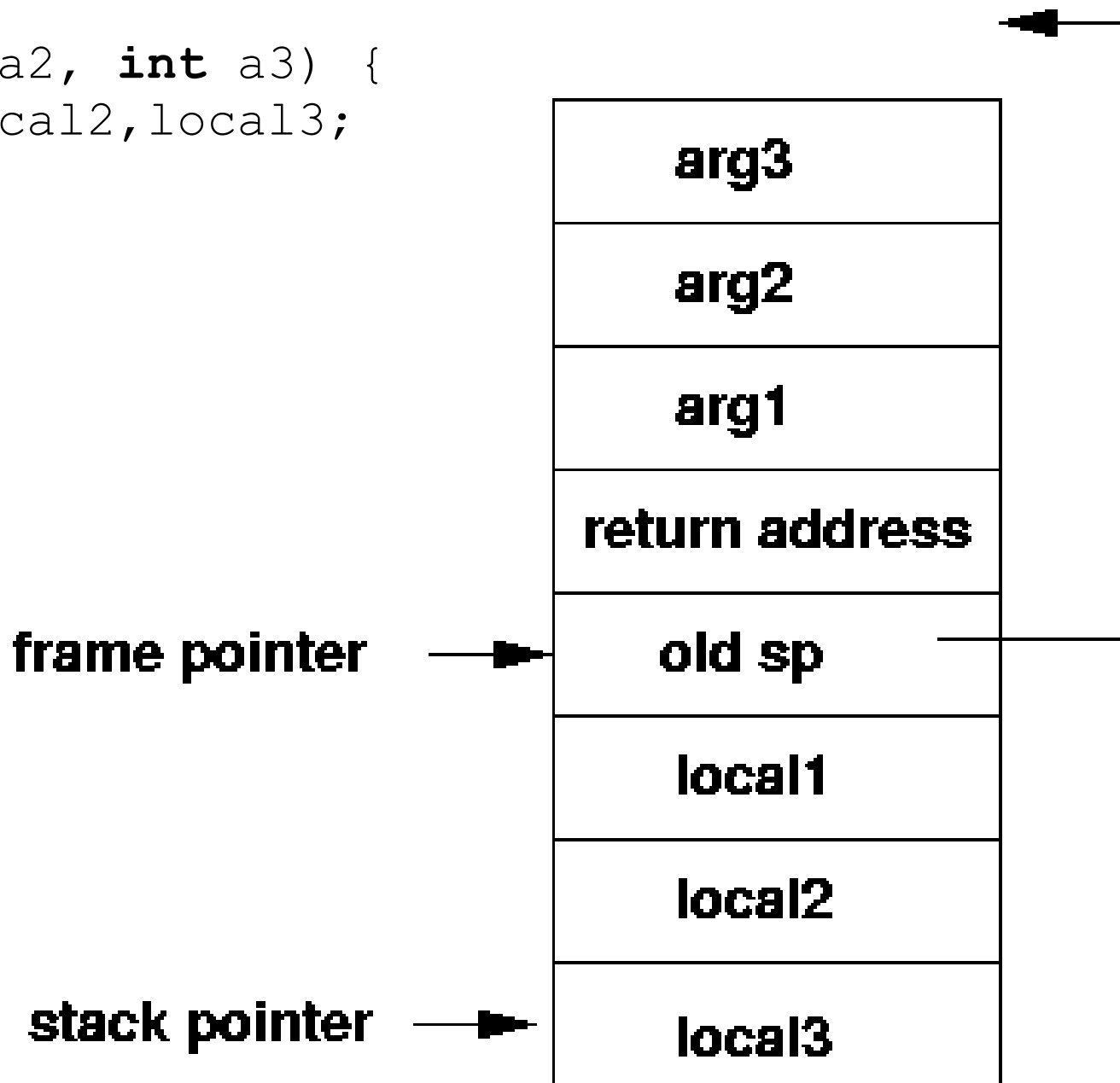
- Adresă fizică

Folosirea memoriei



C/C++ Stack Frame

```
int f(int a1, int a2, int a3) {  
    int local1, local2, local3;  
    ....  
}
```



Exemple

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

void ceva() {
    printf("Hello world!\n");
    exit(0);
}

int main(void)
{
    long * a;
    a = &a + 2;
    *a = ceva;
    return 0;
}
```



Example

```
xor eax, eax
  xor ebx, ebx
  xor edx, edx
  mov dl, 16
  mov al, 4
  mov bl, 1
  push 0x0A21646B
  push 0x726F7720
  push 0x6F6C6C65
  push byte 0x68
  mov ecx, esp
  int 80h
```

```
xor eax, eax
mov al, 1
xor ebx, ebx
int 80h
```

```
31C031DB31D2B210B004B301686B6421
0A6820776F7268656C6C6F6A6889E1CD
8031C0B00131DBCD80
```



Exemple

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

```
char shellcode[] =
```

```
"\x31\xc0\x31\xdb\x31\xd2\xb2\x10\xb0\x04\xb3\x01\x68\x6b\x64\x21"  
"\x0a\x68\x20\x77\x6f\x72\x68\x65\x6c\x6c\x6f\x6a\x68\x89\xe1\xcd"  
"\x80\x31\xc0\xb0\x01\x31\xdb\xcd\x80";
```

```
int main(int argc, char argv[]) {  
    int * a;  
    a = ((char*)&a) + 8;  
    *a = shellcode;  
}
```

Exemple

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

void ceva() {
    printf("Hello world!\n");
    exit(0);
}

int main(void)
{
    long * a;
    a = &a + 2;
    *a = ceva;
    return 0;
}
```



Exemple

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

void ceva() {
    printf("Hello world!\n");
    exit(0);
}

int main(int argc, char * argv[])
{
    char s[4];
    strcpy(s, argv[1]);
    printf("%s\n", s);
    return 0;
}
```



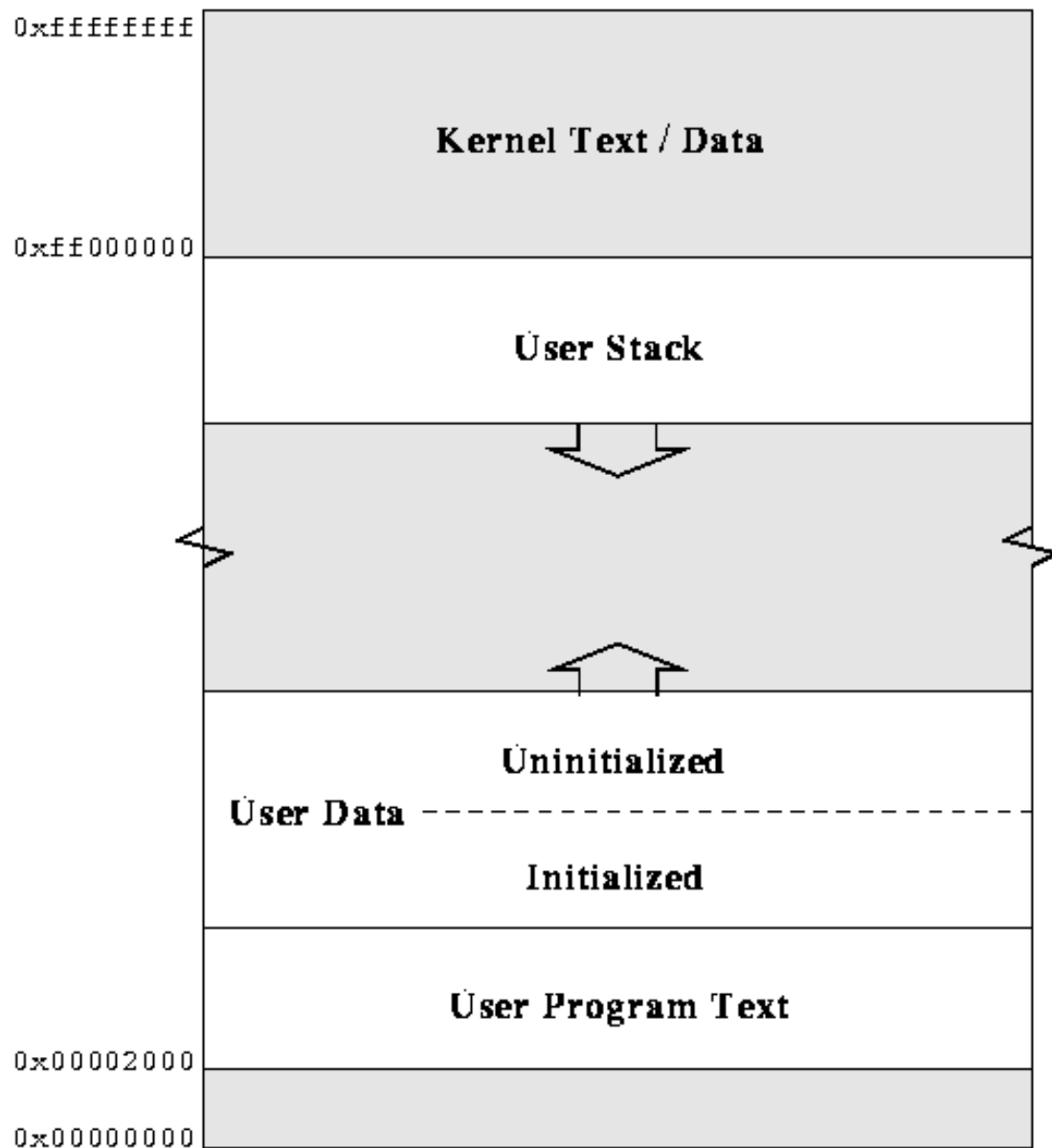
Soluții - canary

```
#include <stdio.h>
#include <stdlib.h>
#define CANARY 0x12345678

void ceva() {
    printf("Hello world!\n");
    exit(0);
}

int main(int argc, char * argv[])
{
    int canary = CANARY;
    char s[4];
    strcpy(s, argv[1]);
    printf("%s\n", s);
    assert(canary == CANARY);
    return 0;
}
```

Soluții - patch



PaX
exec-shield

Vinovații

gets

fgets

sprintf

snprintf

vsprintf

vsnprintf

strcpy

strncpy

strcat

strncat



Vinovații

POLITICA FIRMEI

Closed source

Deadline

Funcționalitate vs securitate

PROGRAMATORUL

Lene

Neatentie

b4dc0d3d

Sfârșit



november **WEBSITE**

```
root@november ~ # logout
```

```
Session closed by the remote host.
```