Computer Security
CS381

Software Security

Yuanyuan Zhang 张媛媛

Object and Executable files

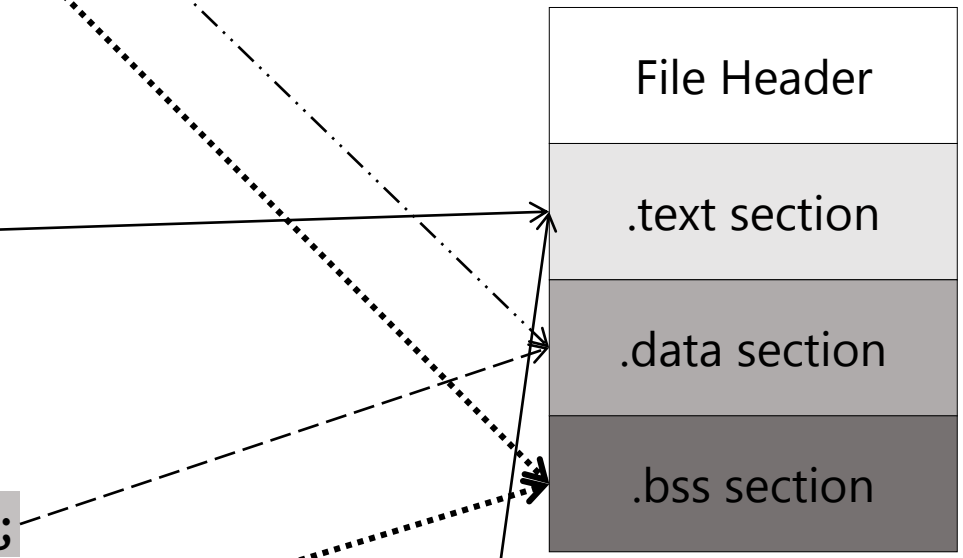
- object.obj
- executable.exe
- dylibrary.dll
- stclibrary.lib

Windows：PE格式
Portable Executable

- object.o
- executable
- dylibrary.so
- stclibrary.a

Linux：ELF格式
Executable Linkable Format

```
int global_init_var = 84;

int global_unint_var;

void func1( int i )
{
    printf( "%d\n", I );
}

int main(void)
{

    static int static_var1 = 85;

    static int static_var2;

    int a = 1;
    int b;
    func1( static_var1 + static_var2 + a + b );
    return 0;
}
```

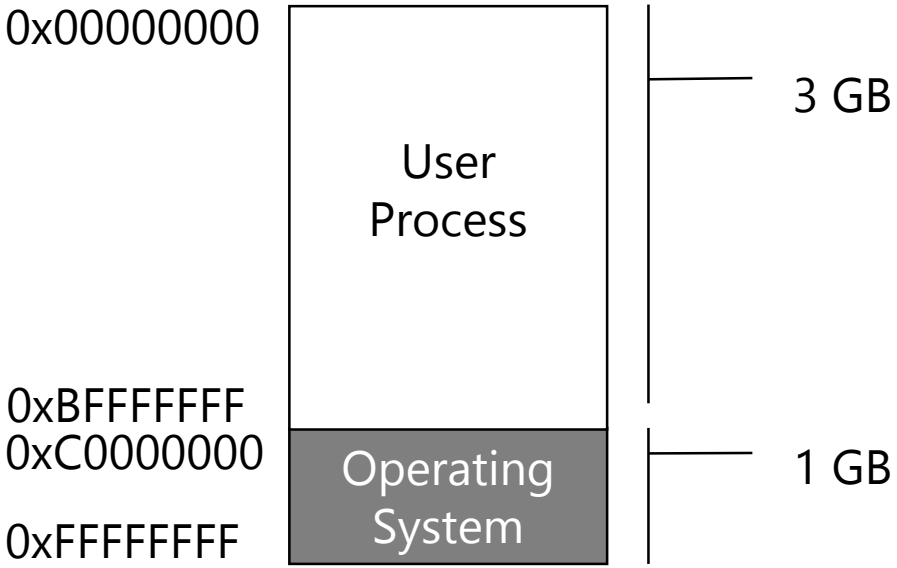


Separation of Code and Data

- **After compiling,**
  a program consists of two segments:
  - Instruction segment：如，代码段
  - Data segment：如，数据段和.bss段

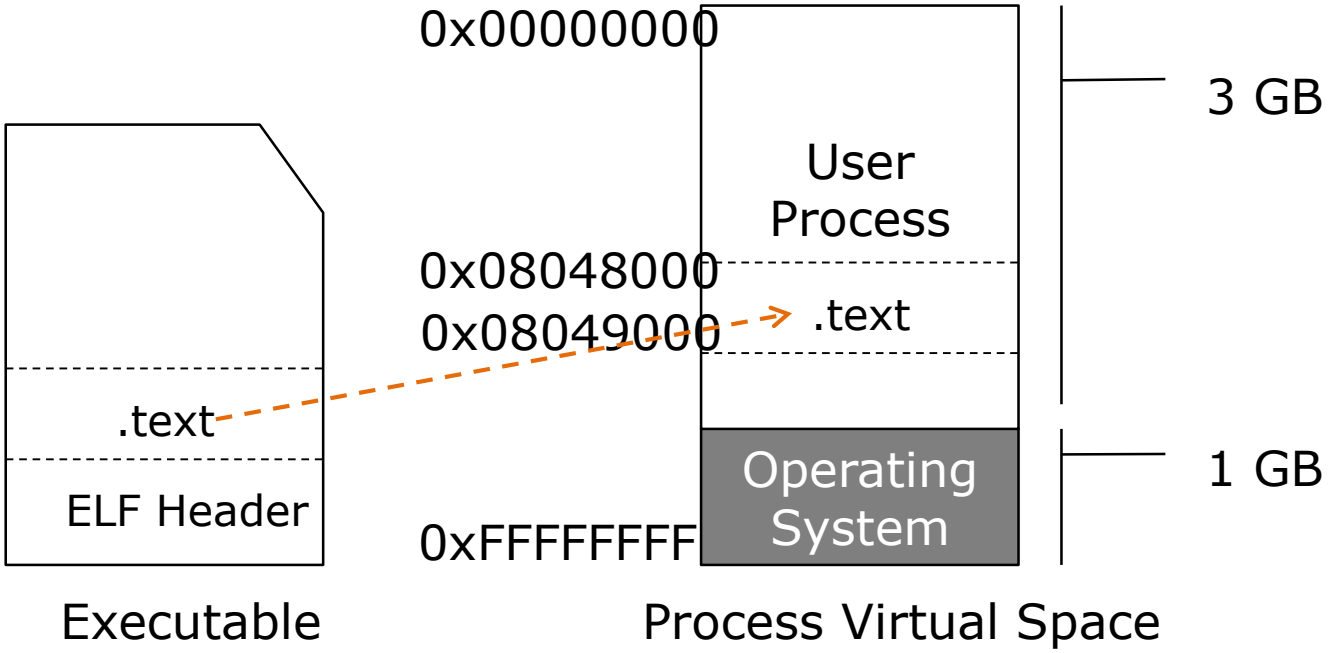
- **Advantages：**
  - Virtual address space mapping 虚拟内存空间映射方便
  - Increasing of locality 提高局部性，增加Cache命中率
  - Sharing the read-only segments 多副本运行时，只读段可共享

Process address space mapping

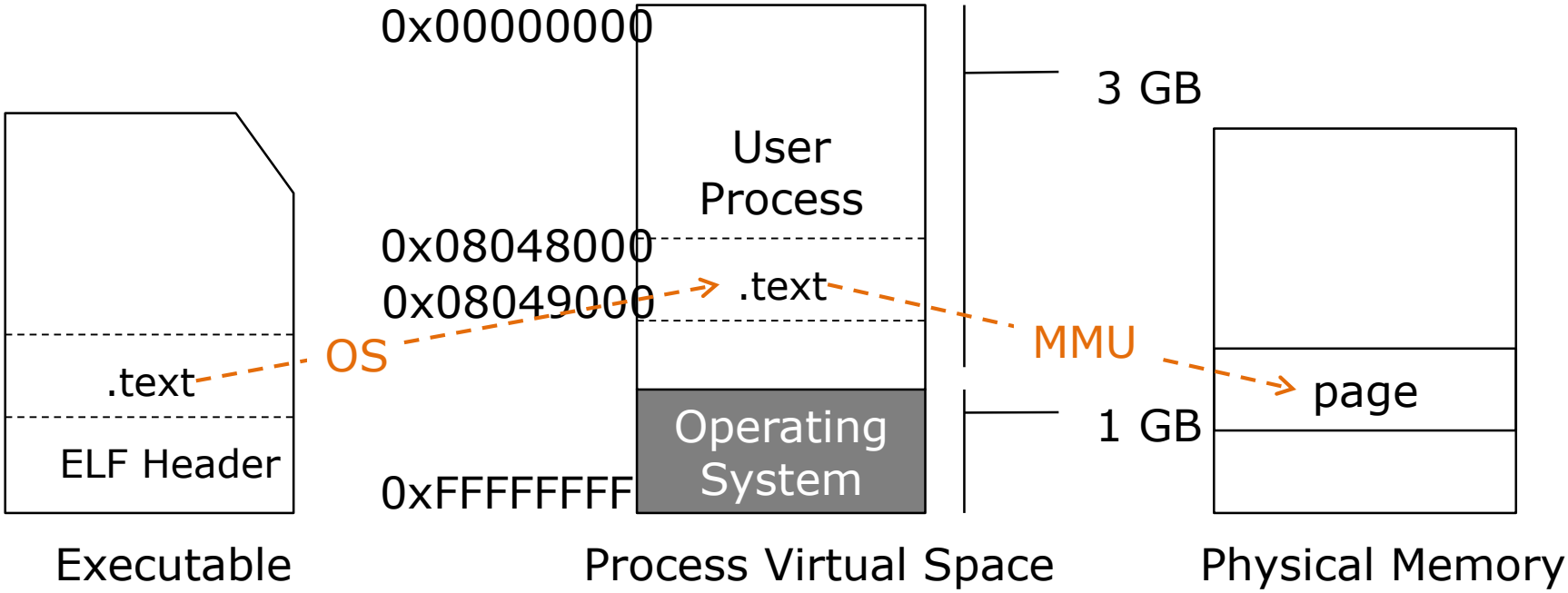


Linux系统下的虚拟地址空间分配

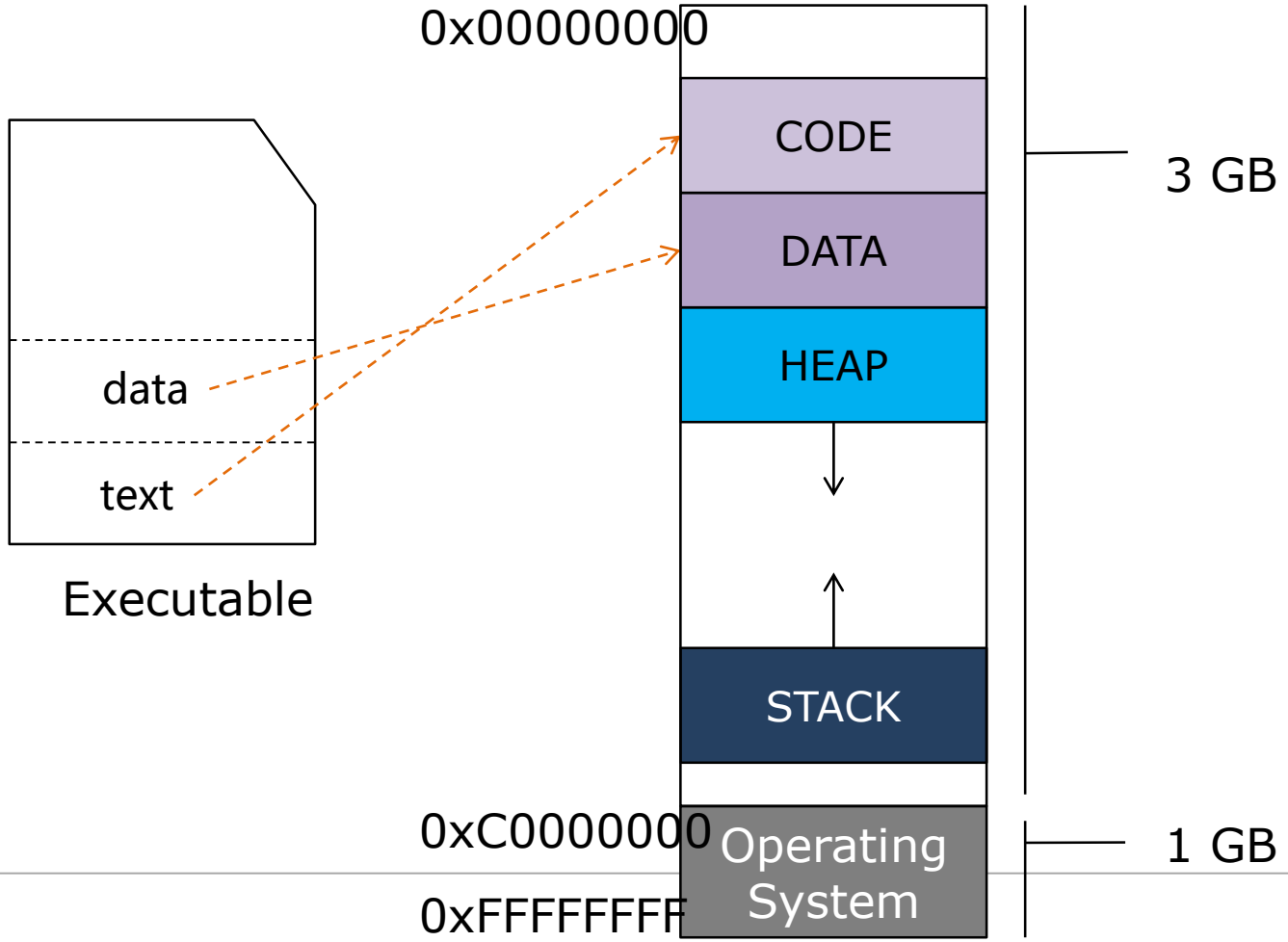
进程虚拟空间的地址映射



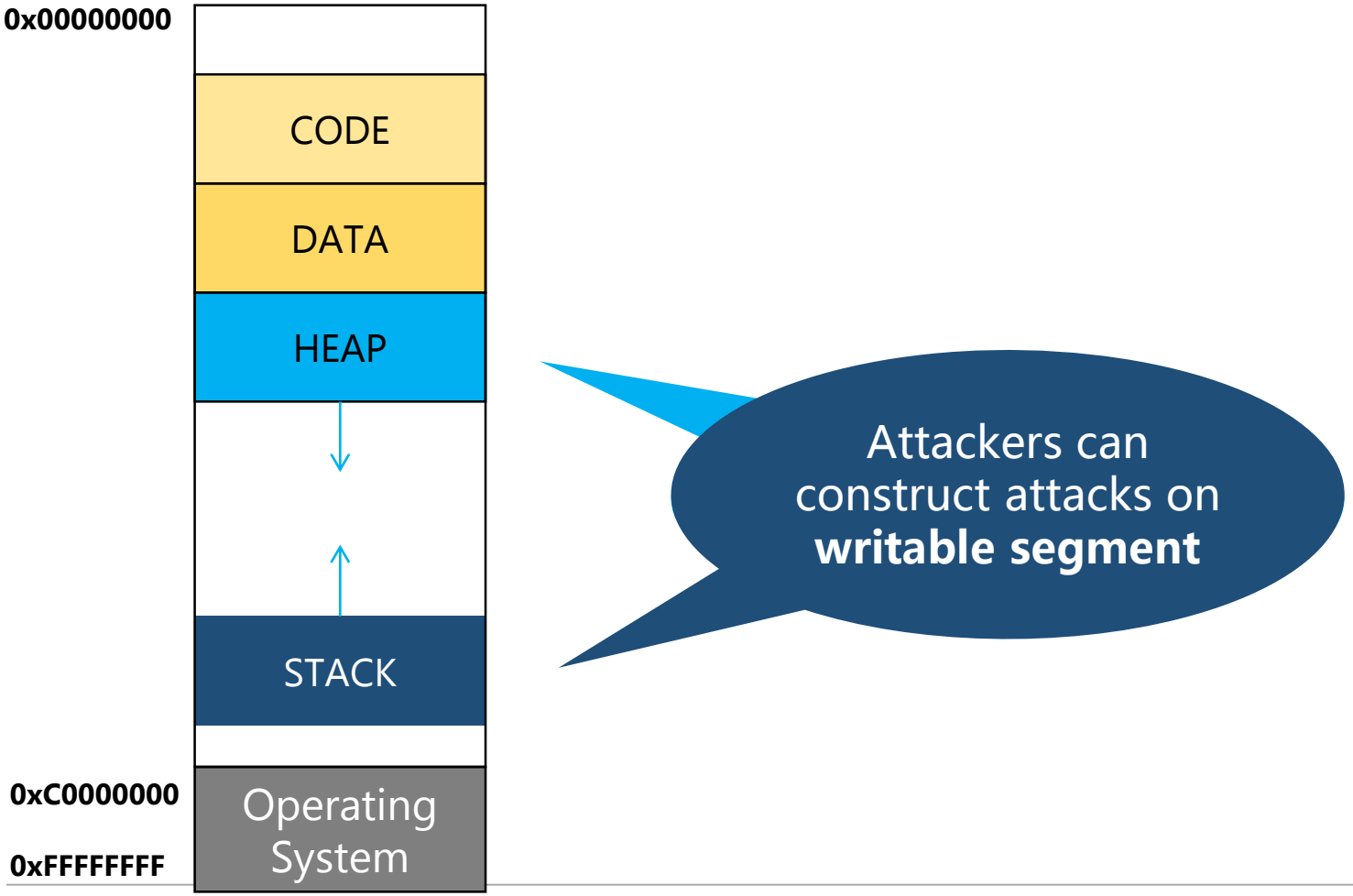
进程虚拟空间的地址映射



虚拟内存空间分布


0x00000000
CODE
DATA
HEAP
STACK
Operating System
0xC0000000
0xFFFFFFFF
3 GB
1 GB
data
text
Executable

Typical attacks

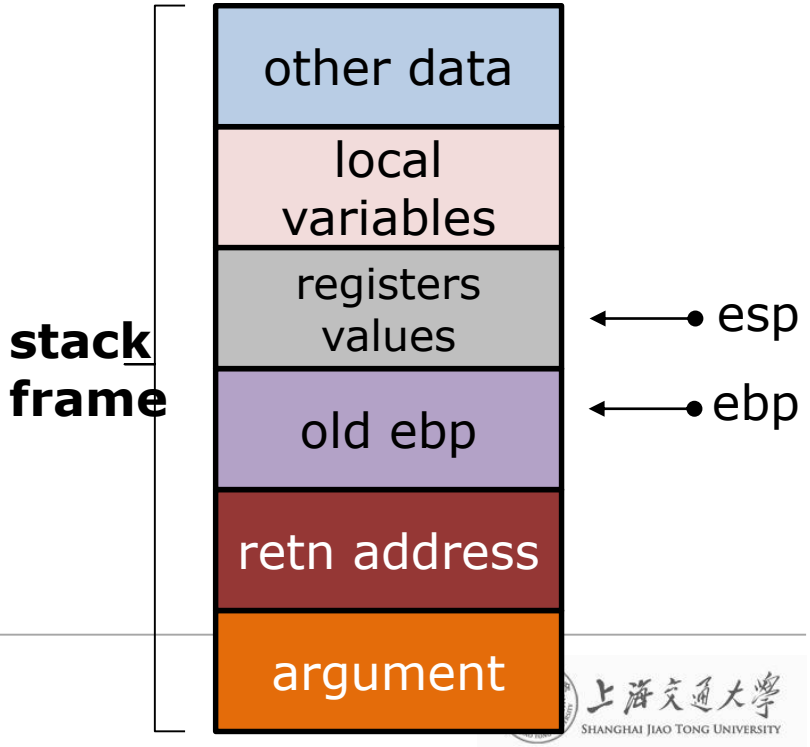


Stack-based attacks 利用栈特性构造的攻击

- **Stack buffer overflow attack**
  - Stack smashing
  - Information leakage

Stack buffer overflow 1: Stack smashing

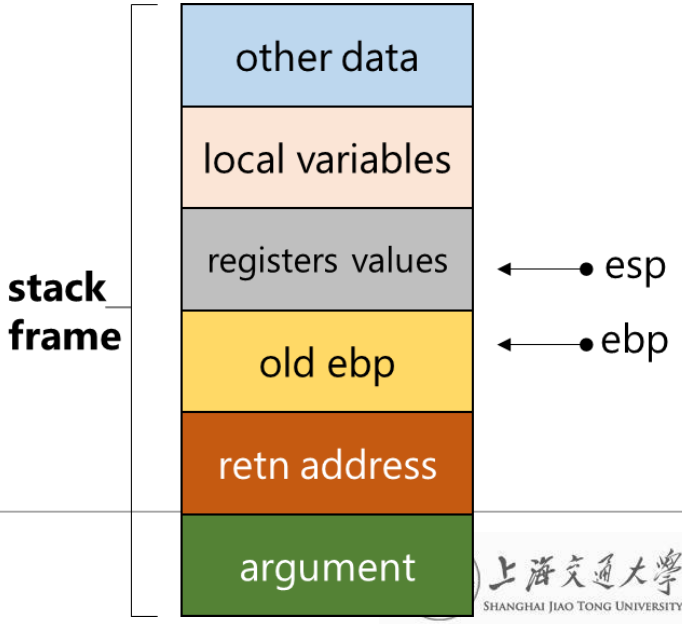
```c
#include <string.h>

void foo (char *bar)
{
    char c[12];          // no bounds checking
    strcpy(c, bar);
}

int main (int argc, char **argv)
{
    foo(argv[1]);
}
```



Stack buffer overflow 2: Information leakage

```
char outstring[80] = "\x10\x01\x48\x08_%08x.%08x.%08x.%08x.%08x|%s|";
printf(outstring);
```

```
outstring[0c]                 // etc...
outstring[08] 0x30252e78      // from "x.%0"
outstring[04] 0x3830255f      // from "_%08"
outstring[00] 0x08480110      // from the ""\x10\x01\x48\x08"
```



Virus, Trojan horse, and Worm

- Virus: computer code that **replicate** itself by modifying other files or programs to insert code that is capable of further replication.

- Trojan horse: malware program that appears to perform some useful task, but which also does something with negative consequences

- Worm: malware program that spreads copies of itself without the need to inject itself in other programs, and usually without human interaction.

Computer Security at a glance

- Physical security
- Operating system security
- Malware
- Network security
- Web security