操作系统安全

清华大学

本章的内容组织

第一节
基础攻击方案

- 内存管理基础
- 内存栈区攻击方案
- 内存堆区攻击方案

内存为对象的攻击
以内存为对象的简单攻击方案

第二节
基础防御方案

- W^X (NX, DEP)
- ASLR
- Stack Canary
- SMAP, SMEP

内存粒度的防御方案
防御基础内存攻击的方案

第三节
高级控制流劫持技术

- 进程执行细节
- 面向返回地址编程
- 全局偏置表劫持
- 虚假vtable劫持

恶意修改进程行为
基于第一章的攻击绕过第二章基础防御

第四节
高级系统保护方案

- 控制流完整性
- 指针完整性
- 信息流控制
- I/O子系统保护

系统粒度的防御方案
通过更严格的安全机制防御控制流劫持

有效防御

成功绕过

有效防御

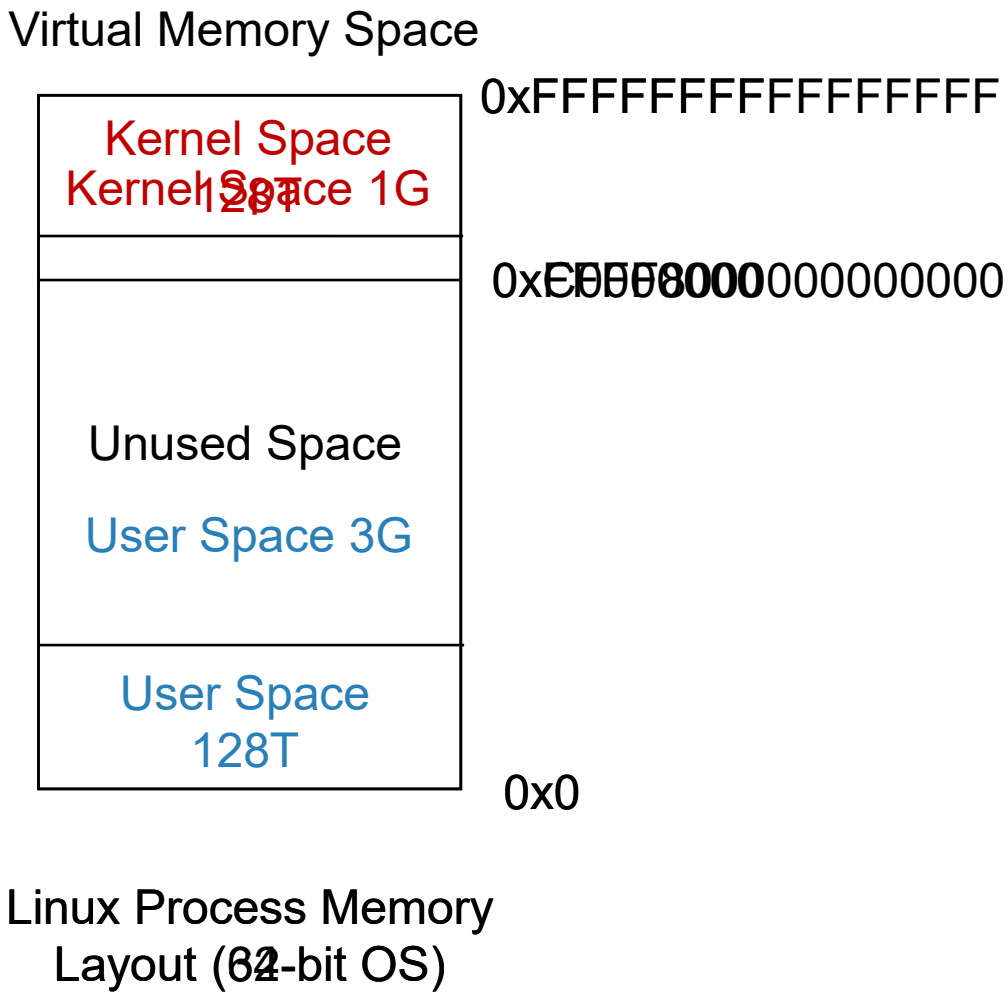
第1节 操作系统基础攻击方案

- **1.1 操作系统内存管理基础**
- 1.2 基础的栈区攻击方案
- 1.3 基础的堆区攻击方案

进程角度的内存管理

- Linux 内核为每一个进程维护一个**独立的**线性逻辑地址空间，以便于实现进程间内存的相互隔离

- 这一线性逻辑地址空间被分为**用户空间**和**内核空间**；用户态下仅可访问用户空间，系统调用提供接口以访问内核空间；内核态下亦无法访问用户空间

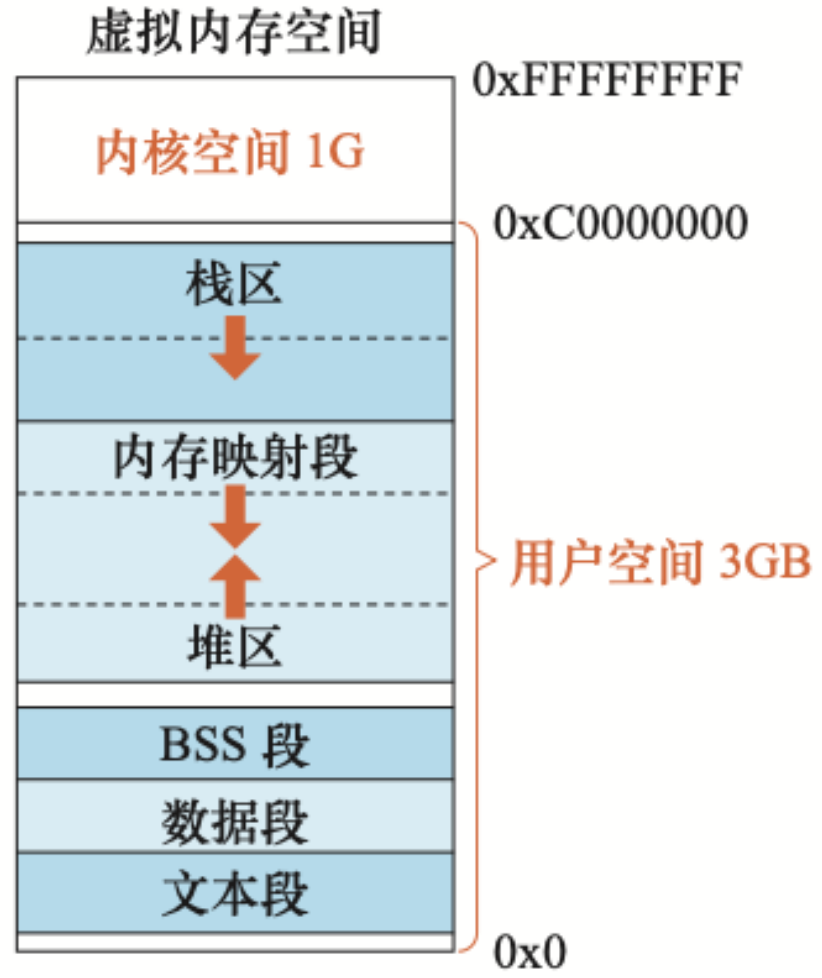


注. 右图为Linux当中内核区与用户区在进程虚拟地址空间下的分布

进程角度的内存管理

用户区内存空间包含了6个重要区域：

1. 文本段：进程的可执行二进制源代码
2. 数据段：初始化了的静态变量和全局变量
3. BSS段：未初始化的静态变量和全局变量
4. 堆区　：由程序申请释放
5. 内存映射段：映射共享内存和动态链接库
6. 栈区　：包含了函数调用信息和局部变量



Linux Process Memory Layout (32-bit OS)

注. 右图为Linux当中用户区的划分方式

内存的权限管理

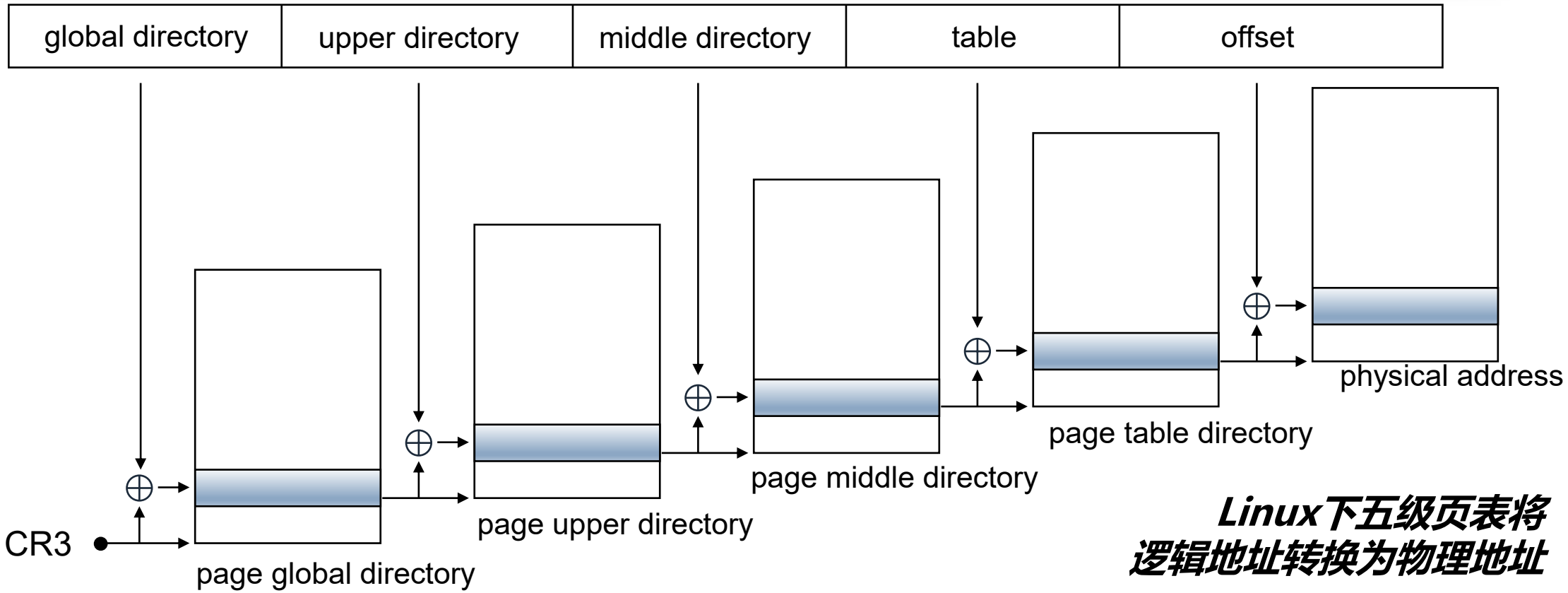
- 用户区内存区域之间的比较：

Question:
为什么文本段只读？

区域名称	存储内容	权限	增长方向	分配时间
文本段	二进制可执行机器码	只读	固定	进程初始化
数据段	初始化了的静态、全局变量	读写	固定	进程初始化
BSS段	未初始化的静态、全局变量	读写	固定	进程初始化
堆区	由进程执行的逻辑决定	读写	向高地址	堆管理器申请内核分配
内存映射段	动态链接库、共享内存的映射信息	内容相关	向低地址	运行时内核分配
栈区	函数调用信息与局部变量	读写	向低地址	函数调用时分配

虚拟地址到逻辑地址的转换

需要注意的是，上述分区均存在于**虚拟地址空间**当中，进程可见的地址均为虚拟地址，内存物理地址对进程不可见；虚拟地址需要经过**页式内存管理模块**才可转换为物理地址，本节提到地址**均为逻辑地址**



Linux下五级页表将逻辑地址转换为物理地址

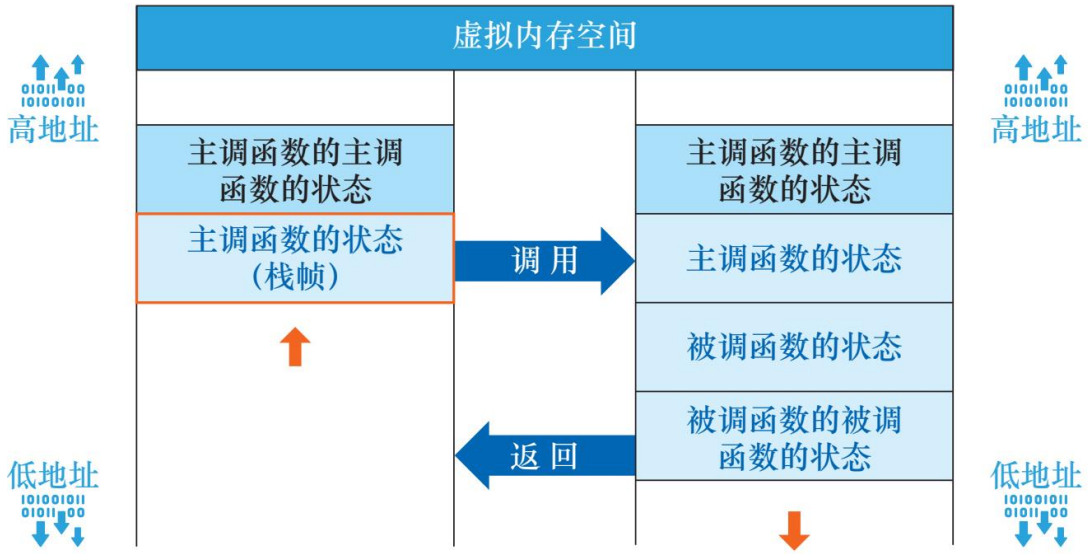
第1节 操作系统基础攻击方案

- 1.1 操作系统内存管理基础
- **1.2 基础的栈区攻击方案**
- 1.3 基础的堆区攻击方案

栈区内存的作用

- 进程的执行过程可以看作一系列函数调用的过程，**栈区内存的根本作用：**

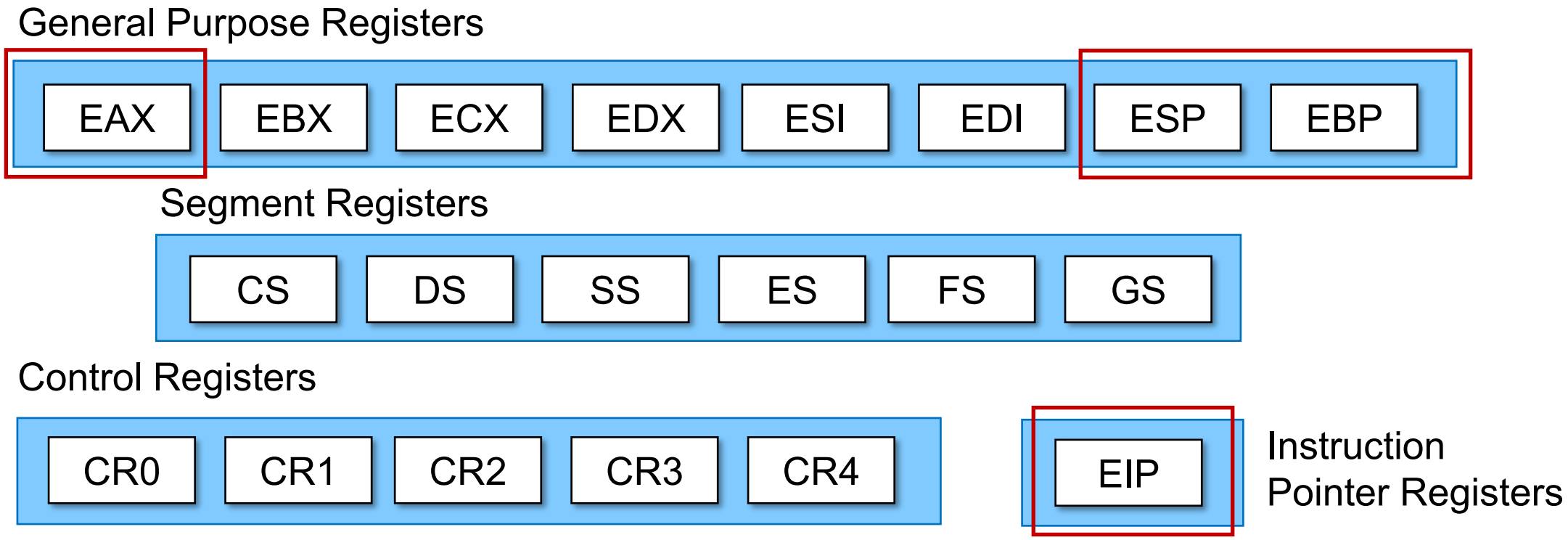
保存主调函数（Caller）的状态信息
以在调用结束后恢复主调函数状态
并创建被调函数(Callee)的状态信息



- 保存主调函数状态的连续内存区域被称作**栈帧**（Stack Frame）；当调用时栈帧进栈，当返回时栈帧出栈；栈帧是调用栈的最小逻辑单元

与函数调用密切相关的寄存器

- 为表示方便，本小节以x86_32处理器下GCC编译程序的调用过程为例，介绍保存和恢复状态的过程
- x86_32下有8个通用寄存器（位宽32），6个段寄存器（位宽16），5个控制寄存器（位宽32），1个指令寄存器（位宽32），和浮点寄存器调试寄存器等



与函数调用密切相关的寄存器

- 我们关注与函数调用相关的四个寄存器：
- 3个通用寄存器：ESP（Stack Pointer）记录栈顶的内存地址
  EBP（Base Pointer）记录当前函数栈帧基地址
  EAX（Accumulator X）用于返回值的暂存

- 1个控制寄存器：EIP （Instruction Pointer）记录下一条指令的内存地址

注. E表示Extend，标记32位寄存器以区别于8086当中的16位寄存器

栈区溢出攻击

栈区溢出攻击

是一种攻击者越界访问并修改栈帧当中的返回地址，
以控制进程的攻击方案的总称

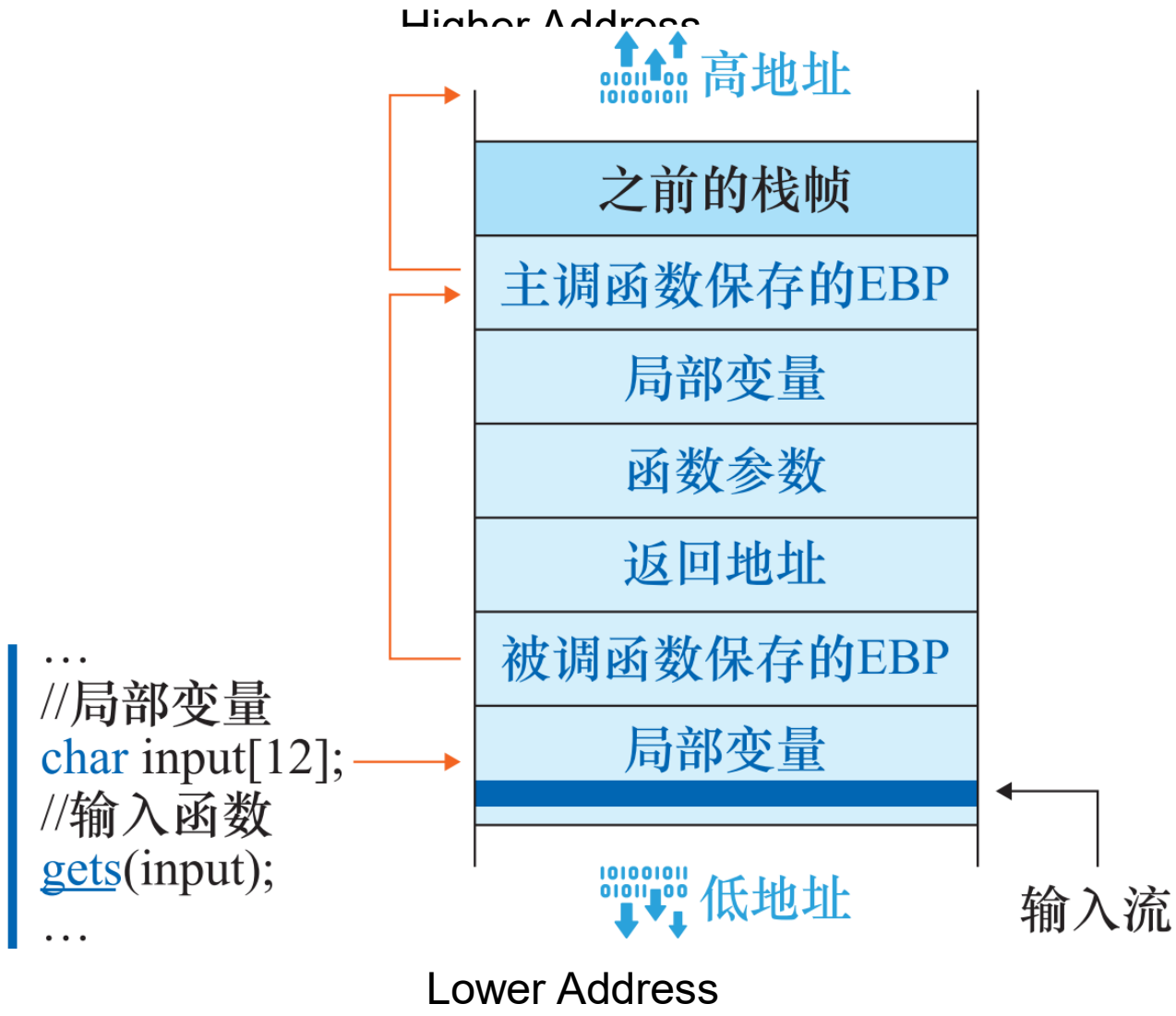
- 栈溢出攻击有多个分类和变体，但其本质均是对于**栈帧中返回地址的修改**，导致**EIP寄存器指向恶意代码**
- 下面假设在**没有任何内存防御机制**的条件下，介绍2个最简单的栈溢出攻击案例

栈区溢出攻击

- **简单的栈区溢出示例1：返回至溢出数据**

1. 攻击者发现可被利用的危险输入函数和可越界访问内存的变量

例如：著名的莫里斯蠕虫病毒就是利用了缺乏输入长度检查的gets函数



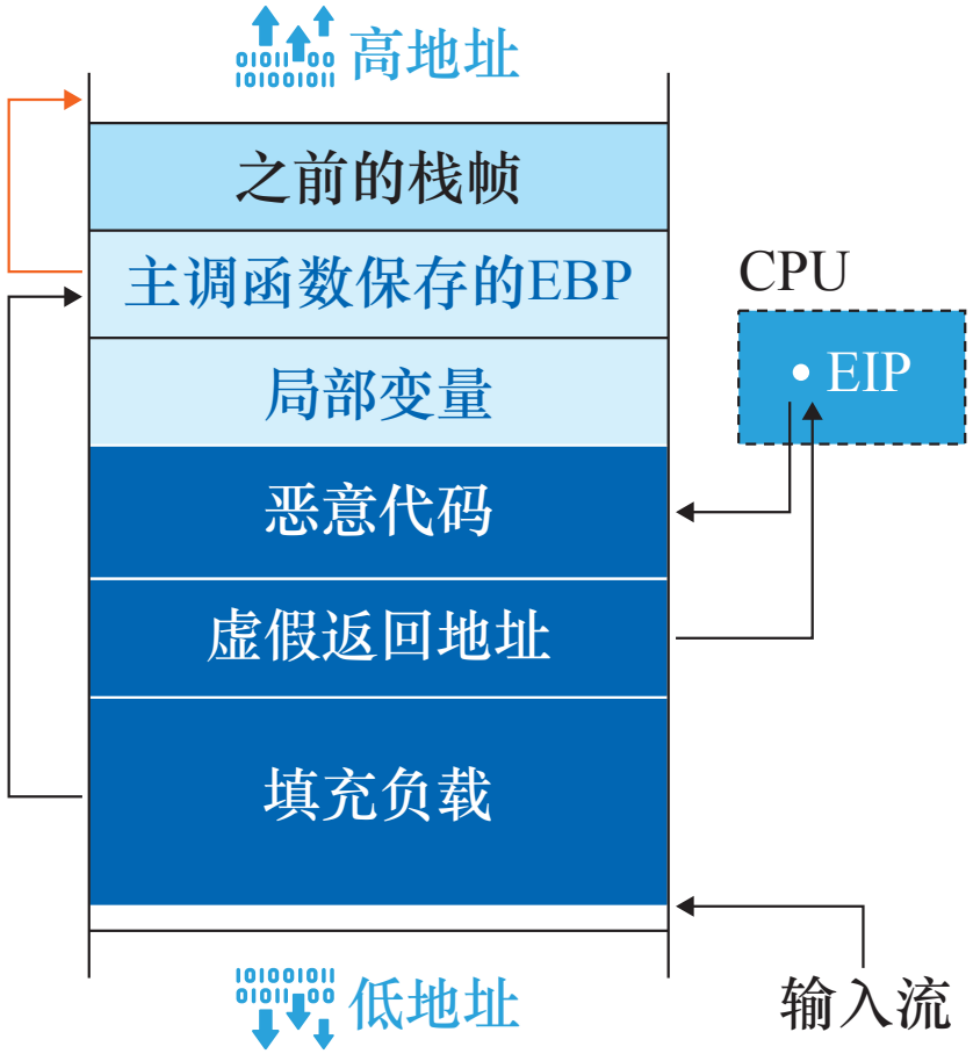
栈区溢出攻击

- **简单的栈区溢出示例1：返回至溢出数据**

2. 确定越界访问变量与返回地址的位置关系

局部变量存储于栈区，栈的增长方向向低地址，因而可以从变量地址加正向偏移访问返回地址

攻击者构造一个填充输入，以覆盖局部变量到返回地址间的内存，并覆盖掉返回地址



栈区溢出攻击

- **简单的栈区溢出示例1：返回至溢出数据**

3. 攻击者构造一段恶意代码，并设置返回地址为恶意代码开始的位置，恶意代码将在函数返回后被执行

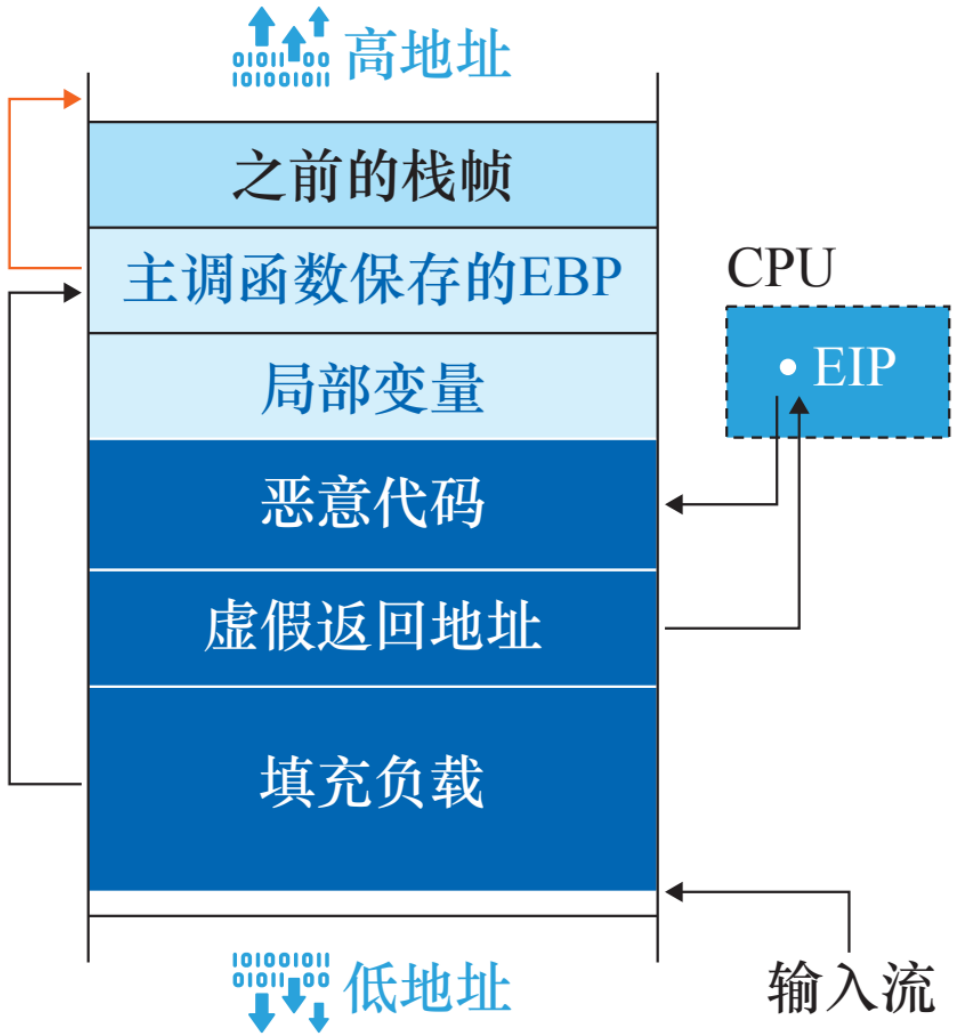
- **最终构造的恶意的输入分为三个部分：**

a. 局部变量到返回地址间的恶意填充

b. 返回地址的覆盖值

c. 恶意的代码段

此外，攻击者也可以不构造代码段，仅通过输入不存在的返回地址让程序崩溃



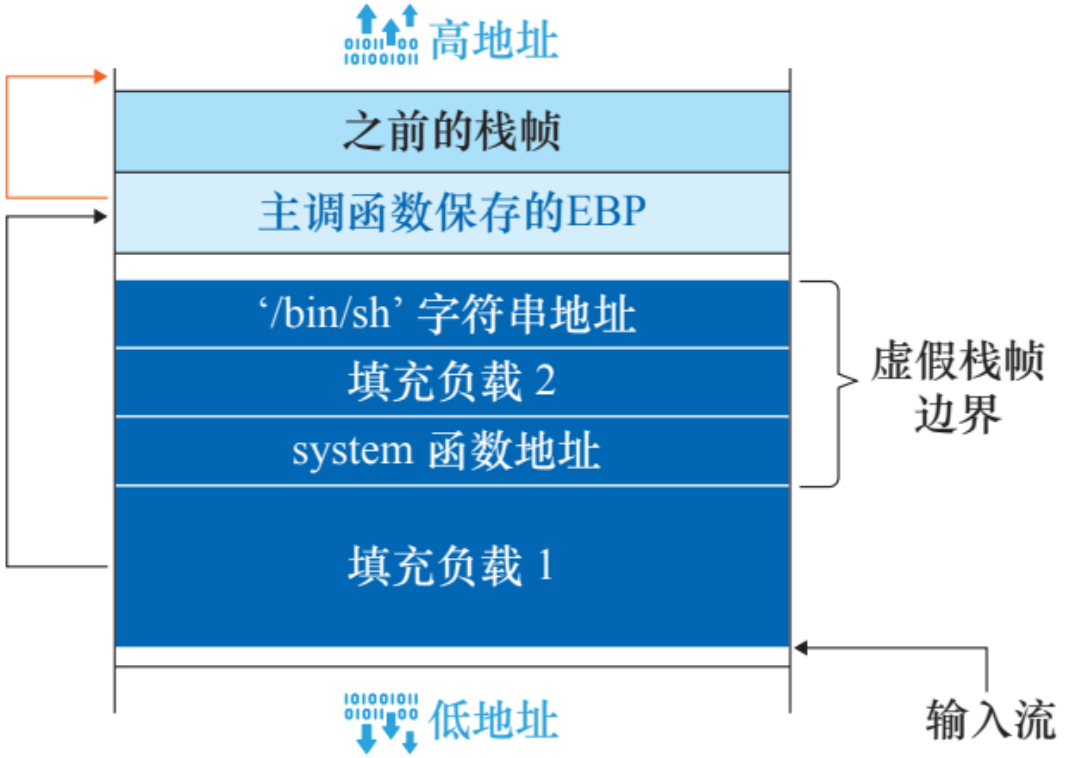
栈区溢出攻击

- **简单的栈区溢出示例2：返回至库函数**

在这个示例当中，攻击者希望进程调用某一动态链接库当中的库函数

假设攻击者希望调用libc的system函数，并传递参数为‘/bin/sh’进而获取操作系统的shell，执行任意指令

攻击者应该如何传递函数调用的参数?



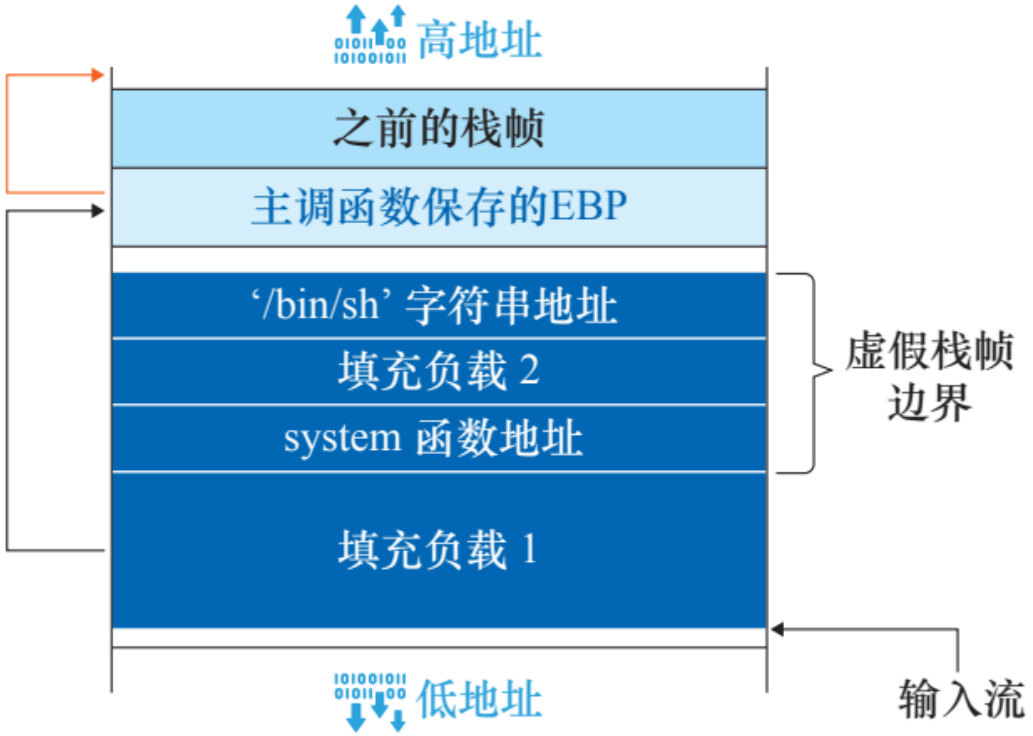
注. 假设内存映射段当中存在system函数

栈区溢出攻击

- **简单的栈区溢出示例2：返回至库函数**

攻击者在受害进程的栈区伪造
一个**栈帧的边界**

总体来说，攻击者在恶意输入当中构造了一个函数调用时的内存结构；
当进程返回时到system函数当中执行，system函数在高地址当中找到伪造的函数参数，完成恶意的函数调用过程



注. 靠上的padding payload 2的作用是填充返回地址的位置，相当于恶意调用system函数后的返回地址

栈区溢出攻击总结

- **以上简单的栈溢出攻击的局限性**

以上简单的栈溢出攻击在现实操作系统环境下几乎无法成功；为防御栈区溢出，已有诸多内存级别的保护机制，例如NX、ASLR、Stack Canary、DEP等将在第二节当中介绍

- 栈区溢出攻击是被最广泛使用的控制流劫持手段，我们将在第三节当中详细讨论**以栈溢出为基础**的复杂进程控制流劫持方案，并绕过基础操作系统防御机制

第1节 操作系统基础攻击方案

- 1.1 操作系统内存管理基础
- 1.2 基础的栈区攻击方案
- **1.3 基础的堆区攻击方案**

堆区溢出攻击

堆溢出攻击

是一类攻击者越界访问并篡改堆管理数据结构，实现恶意内存读写的攻击

- 堆区溢出攻击是堆区最常见的攻击方式，这种攻击方式可以实现恶意数据的覆盖写入，进而实现进程控制流劫持

堆溢出的使用广泛，25%针对windows7的攻击都是堆区溢出

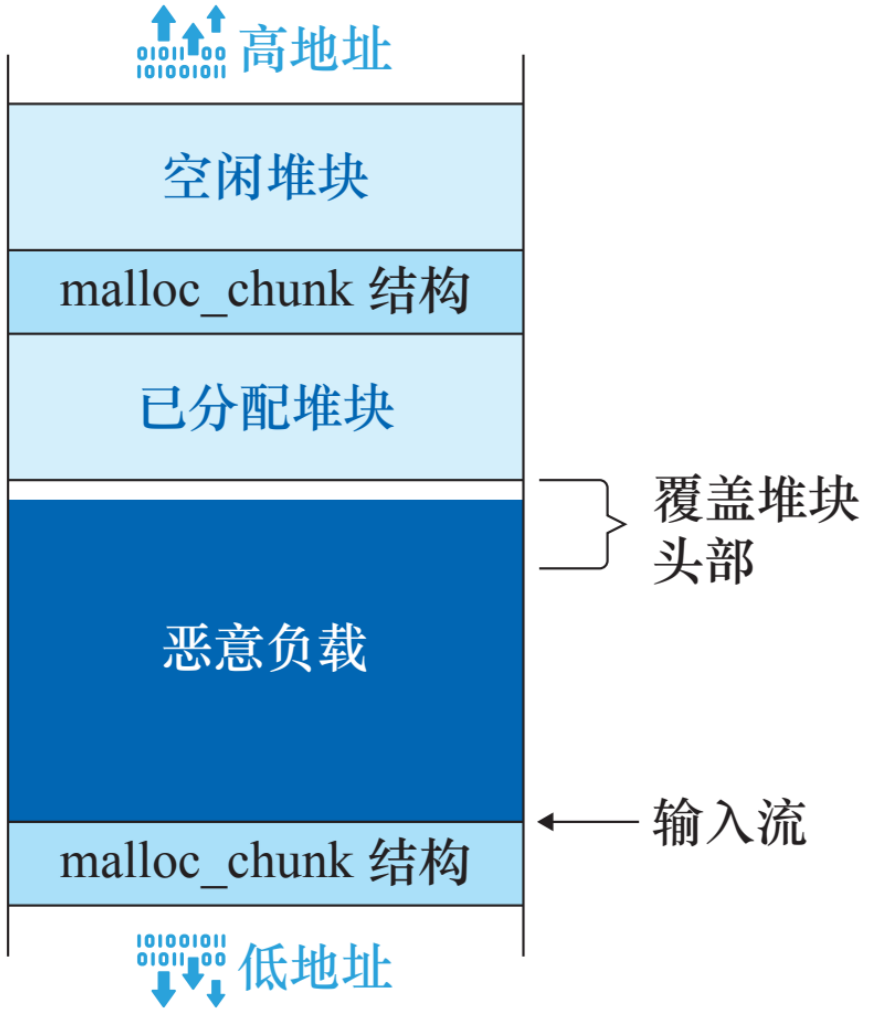
Heap Vulnerability	Occurrences
Heap Overflow	673
Use-After-Free	264
Heap Over-Read	125
Double-Free	35
Invalid-Free	33

注. 数据来自CVE-2017当中的检索结果

堆区溢出攻击

- **最简单的堆区溢出：**

直接覆盖malloc_chunk首部为无意义内容，在堆管理器处理管理元数据时将造成崩溃

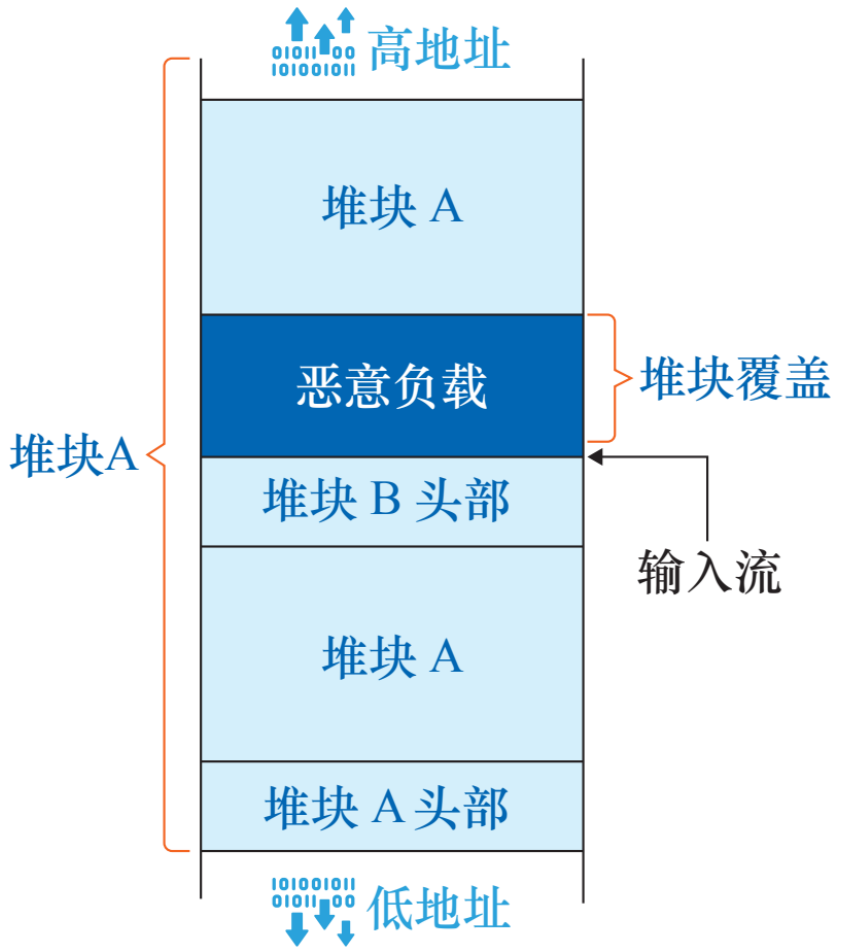


堆区溢出攻击

- **堆区溢出：构造堆块重叠（Heap Overlap）**

堆块重叠是一种**病态**堆区内存分配状态，
同一堆区逻辑地址被堆管理器**多次分配**

如右图所示，造成Heap Overlap之后攻击者可以通过写入一个堆块，实现对另一堆块内容的写入；同理，读出被覆盖堆块当中的数据



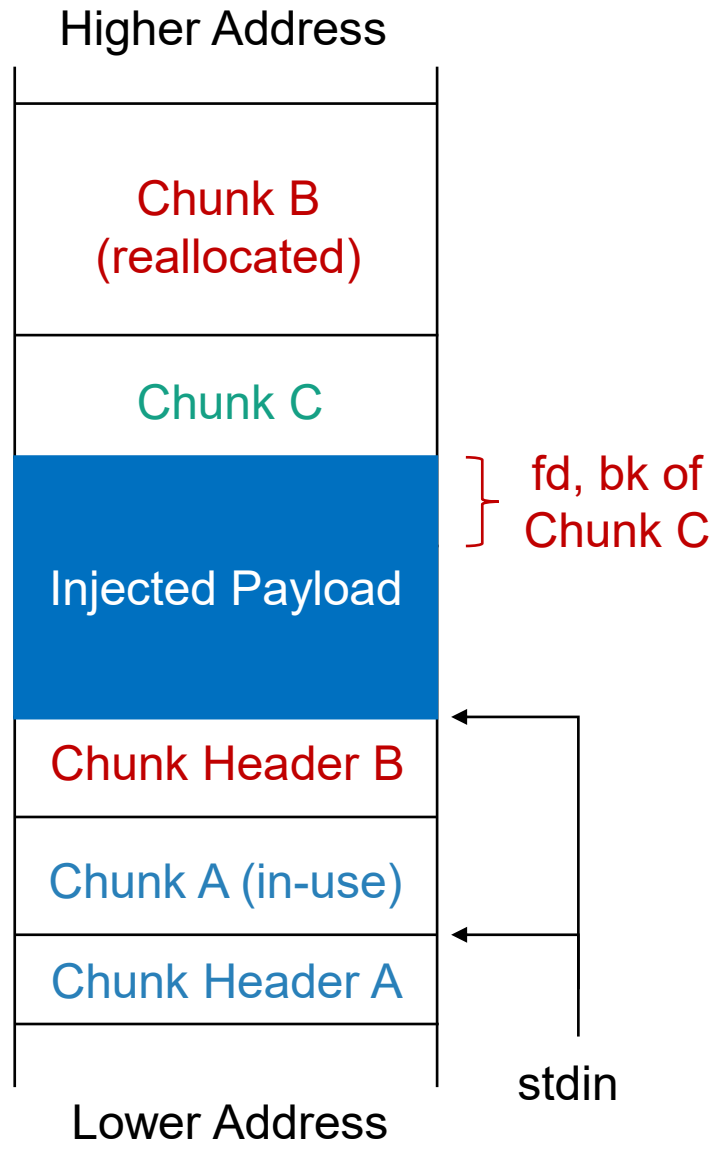
堆区溢出攻击

- **更加复杂的堆区溢出攻击：利用堆管理其他机制**

例如，基于unlink机制的堆区溢出攻击：

unlink宏从**空闲堆块构成的双向链表**中，提取**空闲堆块**，而后返回给用户**空闲堆块**

攻击者将设法用溢出数据**覆盖前/后向链表指针**（fd，bk字段），在unlink宏调用时可以将任意内存地址当作未分配的堆块使用；
最终，攻击者可**读/写任意内存区域**（write-anything-anywhere），并以此为基础进行更复杂的攻击

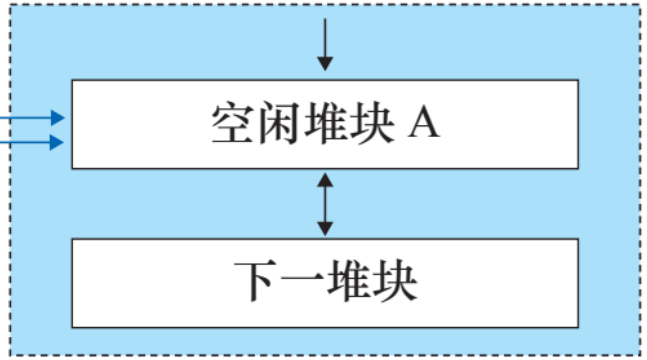


堆区的其他攻击：Use-After-Free

- **Use-After-Free** 是进程由于实现上的错误，**使用已被释放的堆区内存**，UAF是一种存在广泛的漏洞，仅2020年上半年，**CVE当中就汇报了超过90种UAF漏洞**

被free函数释放的堆块内存仍然可以被继续使用，当再次调用malloc分配内存时，会同时有两个指针指向同一堆块造成 **堆块重叠**

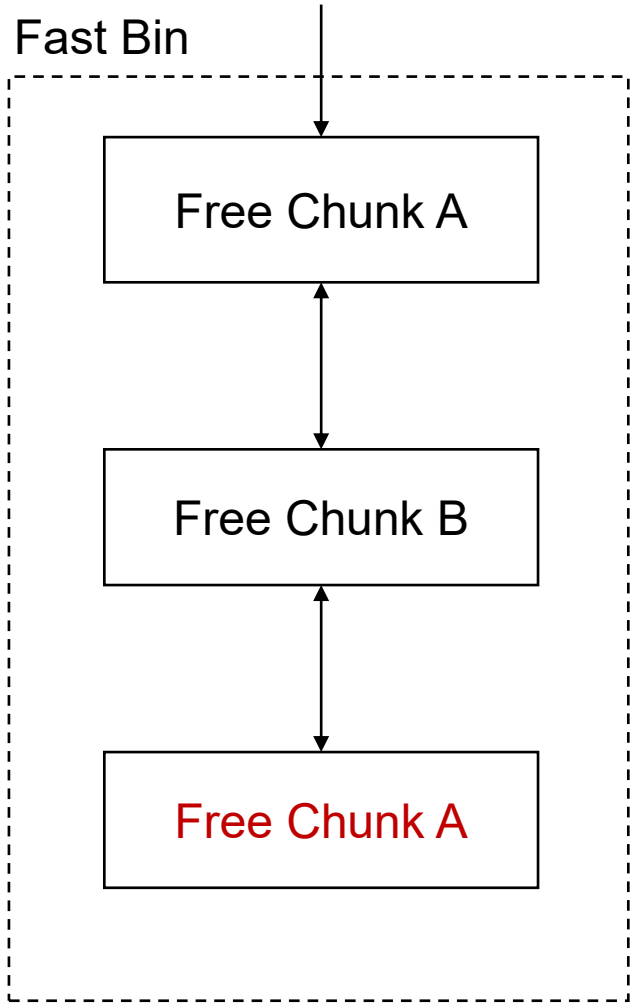
```
// 空悬指针
free(p1);
…
void * p2 = malloc(…);
//已分配堆块 A
```



注. 指向已被释放的内存的指针为空悬指针（Dangling Pointer）

堆区的其他攻击：Double-Free

- Double-Free指的是进程**多次释放统一堆块**，被多次释放的堆块将**被堆管理器分配多次**，最终产生堆块重叠；



Double-Free多发生在Fast-Bin当中，因为Fast-Bin当中的空闲块更倾向于被反复分配与释放

注. Fast-Bin 用于收集较小的空闲堆块（16-80B），方便反复申请小块内存的场景

堆区的其他攻击：Heap Over-read

- 堆溢出攻击越界写入并覆盖堆区数据，而Heap Over-Read则直接越界读出堆区数据，造成信息泄露

著名的Heartbleed Attack是最典型的Heap Over-Read Attack

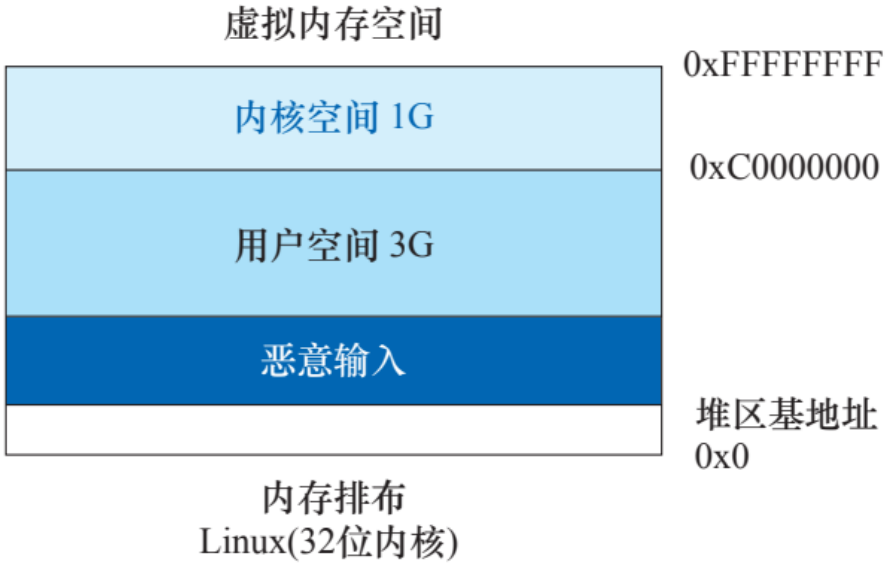
- OpenSSL的TLS实现当中，在处理心跳包时未能对长度字段做合理校验，导致攻击者可以构造恶意数据包，越界读取心跳包数据之后的堆区内存；这些内存包含了私钥等重要信息

该漏洞可倾泻的数据量高达64KB，而Fast-Bin当中的堆块最大大小仅为80B（为其大小的800-4000倍）

堆区的其他攻击：Heap Spray

- 堆喷（Heap Spray）并非是一种内存攻击的辅助技术；堆喷申请大量的堆区空间，并将其中填入大量的**滑板指令**（NOP）和攻击恶意代码；

- 堆喷使用户空间存在大量恶意代码，若EIP指向堆区时将命中**滑板指令区**，受害进程最终将“滑到”恶意代码



堆喷对抗地址的随机浮动类型的防御方案

并实现了恶意代码的注入

第2节 操作系统基础防御方案

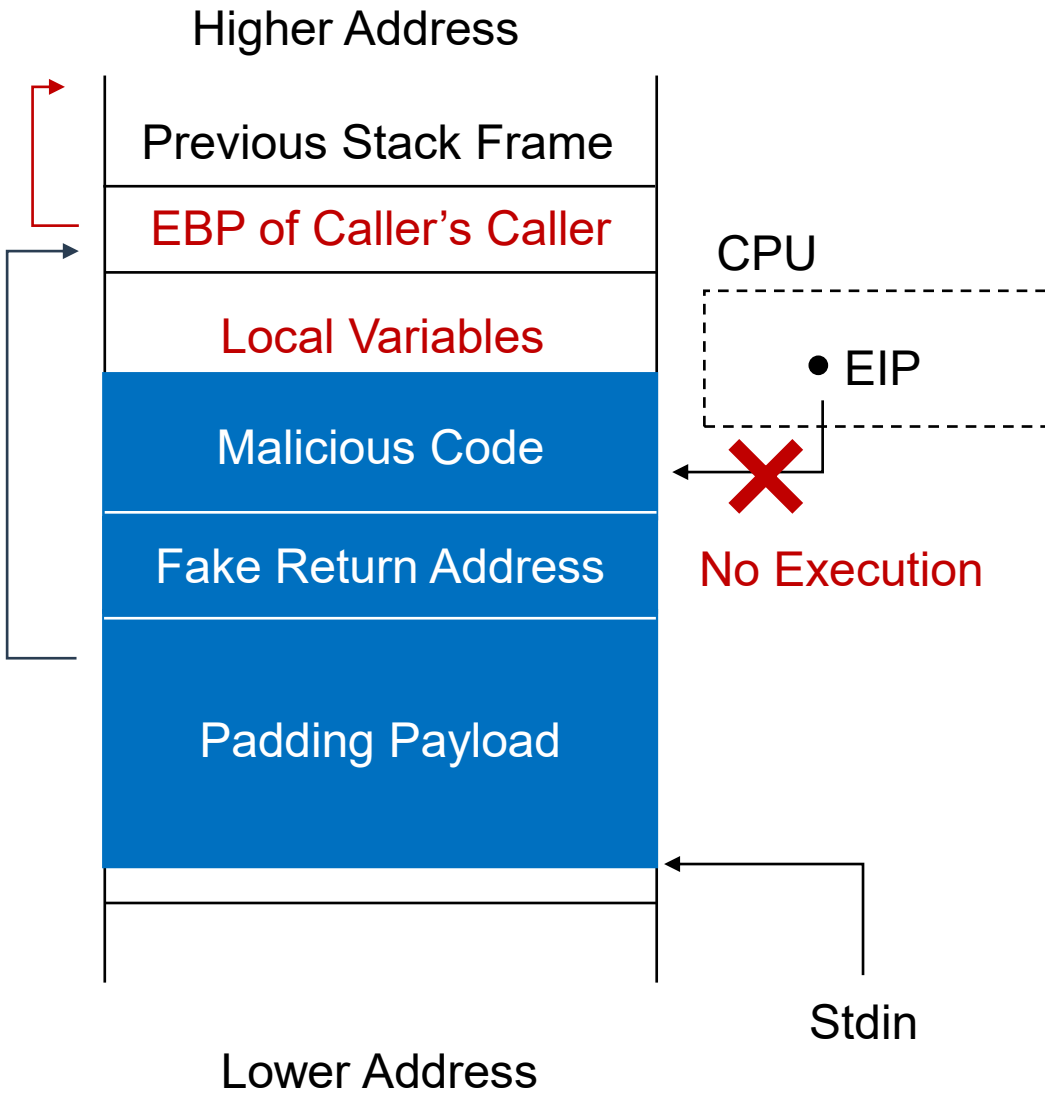
- 2.1 W^X（NX，DEP）
- 2.2 ASLR
- 2.3 Stack Canary
- 2.4 SMAP, SMEP

内存防御技术：W^X

- W^X 是**写与执行不可兼得**，即每一个内存页拥有**写权限或者执行权限**，不可兼具两者

当W^X最早在FreeBSD 3.0当中被实现，在Linux下的别名为**NX**（No eXecution），Windows下类似的机制被称为**DEP**（Data Execution Prevention）

当W^X生效时，**返回至溢出数据的栈溢出攻击**失效，因为无法执行位于栈区的注入的恶意代码；
但仍有方法可以绕过NX保护机制，将在下一节的高级控制流劫持方案中介绍

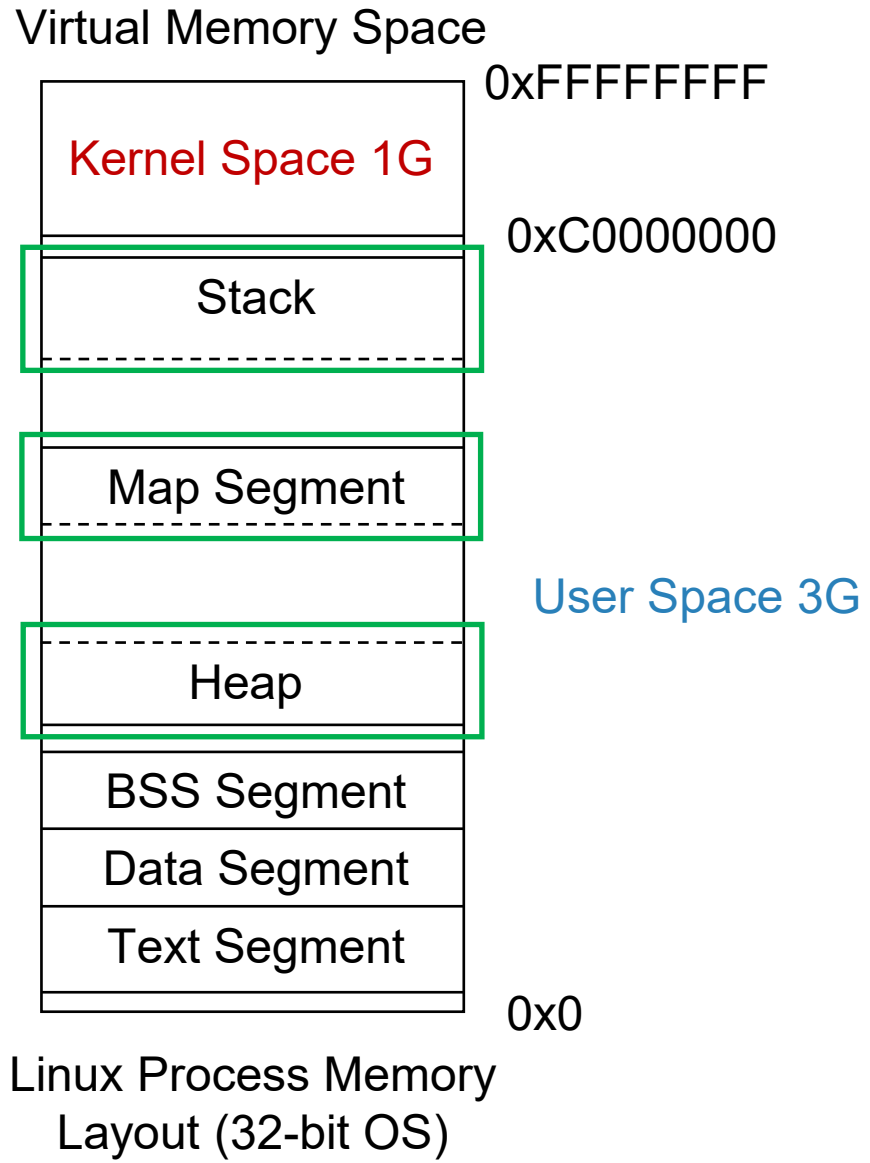


内存防御技术：ASLR

- ASLR（address space layout randomization）是一种对虚拟空间当中的**基地址进行随机初始化**的保护方案；以防止恶意代码定位进程虚拟空间当中的重要地址；目前在各主流操作系统下均有实现

ASLR随机化的对象包含了：

1. 共享库的基地址（.so文件加载的基地址）
2. 栈区的基地址
3. 堆区的基地址



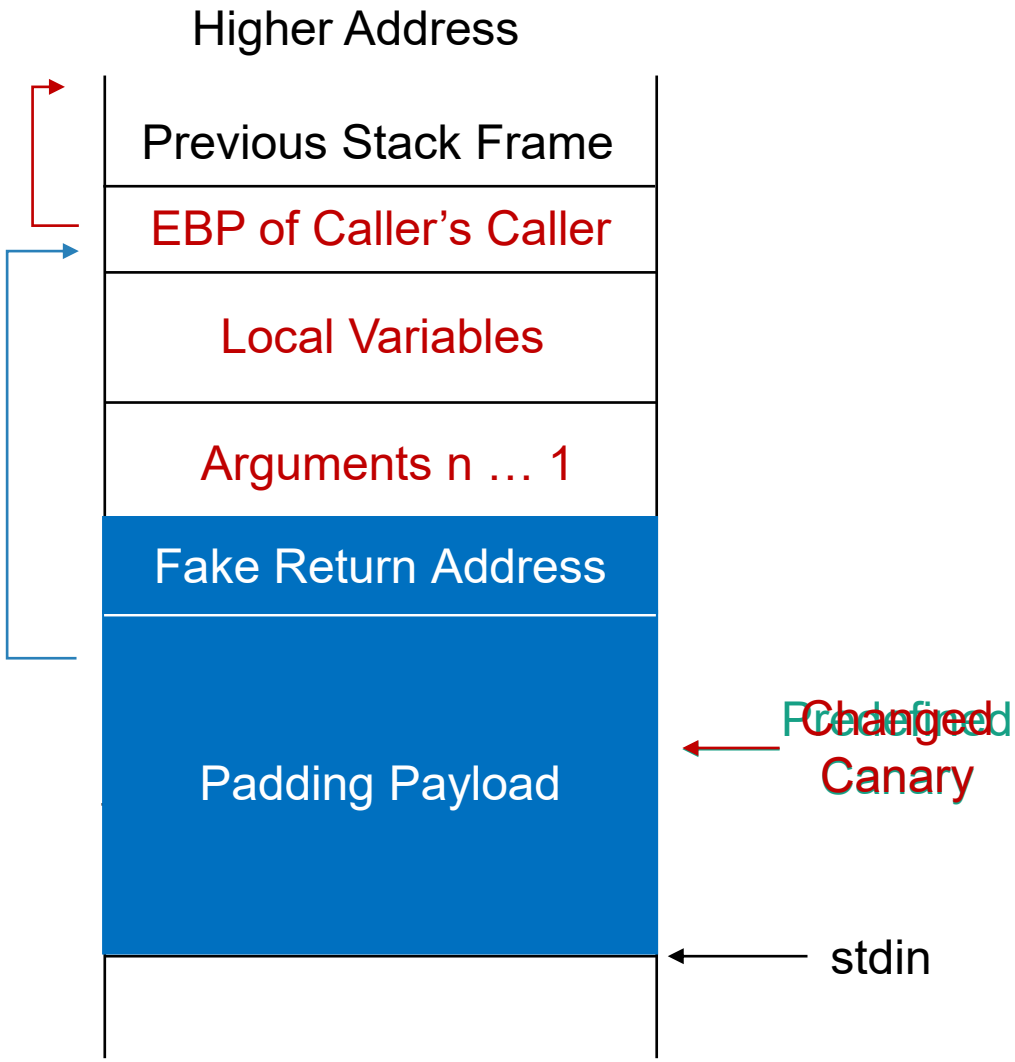
注．ASLR实现需要编译器的PIE支持（Position Independent Executable）才可将代码加载到随机化的地址上

内存防御技术：Stack Canary

- Canary的本意是金丝雀，Stack Canary是一种防御栈区溢出的方案

其本质是，在保存的栈帧基地址（EBP）之后插入一段信息，当函数返回时验证这段信息是否被修改过

当发生栈区溢出时，攻击者为了修改返回地址，必须先覆盖Stack Canary，造成攻击行为暴露



注. 其得名缘由：https://en.wikipedia.org/wiki/Stack_buffer_overflow

内存防御技术：SMAP, SMEP

SMAP和SMEP是两种基础的**内存隔离技术**

- SMAP（Supervisor Mode Access Prevention，管理模式访问保护）禁止内核访问用户空间的数据
- SMEP（Supervisor Mode Execution Prevention，管理模式执行保护）禁止内核执行用户空间代码，是预防**权限提升**（Privilege Escalation）的重要机制

SMAP/SMEP 和 W^X 均需要处理器硬件的支持

内存防御技术总结

- 虽然操作系统提供了大量防御内存攻击的方案，但这些防御方案仍可以被攻击者挫败或绕过：

对于Stack Canary，作为Canary的内容可能被泄露给攻击者，或被暴力枚举破解[1]

对于ASLR已有去随机化方案，泄露内存分布信息[2,3]

在第三节将介绍ROP等进程控制流劫持方案亦可以绕过ASLR、NX的保护机制

1. Wei Wu, et al. "KEPLER: Facilitating Control-flow Hijacking Primitive Evaluation for Linux Kernel Vulnerabilities." 28th USENIX Security Symposium, 2019.
2. Daniel Gruss, et al. "Prefetch side-channel attacks: Bypassing SMAP and kernel ASLR." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security.
3. Ben Gras, et al. "ASLR on the Line: Practical Cache Attacks on the MMU." NDSS. Vol. 17. 2017.

第3节 高级控制流劫持方案

3.1 进程执行的更多细节

3.2 面向返回地址编程

3.3 全局偏置表劫持

3.4 虚假vtable劫持

进程的内核态和用户态

- Linux下进程可处于**内核态**或**用户态**，内核态下拥有更高的指令执行权限（在Intel x86_32下对应ring0）用户态下只拥有低权限（对应ring3）

微处理器在指令执行时，对权限进行严格检查，
管理用户直接访问硬件资源的权限，提升系统的安全性

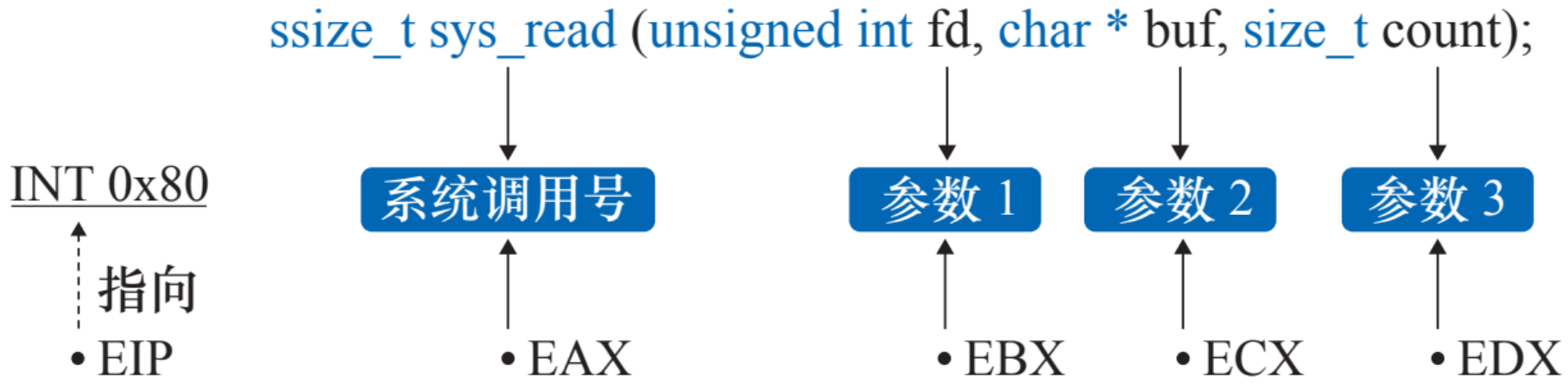
- Linux下内核态与用户态的切换主要由三种方式触发：（1）系统调用（2）I/O设备中断（3）异常执行；其中系统调用是进程主动转入内核态的方法

因而也称系统调用是**内核空间**与**用户空间**的桥梁

进程触发系统调用

- Linux在x86_32架构下触发系统调用的方法：（下图以触发sys_read为例）

1. 将EAX设置为对应的系统调用号
2. 将EBX、ECX等寄存器设置为系统调用参数
3. EIP指向并执行中断触发指令，触发0x80中断



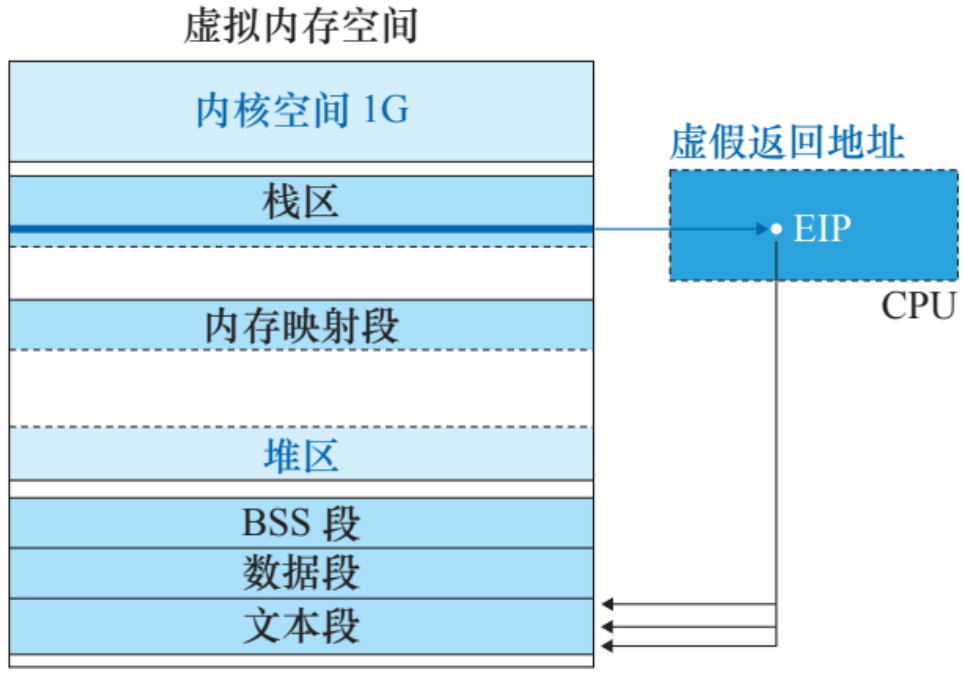
第3节 高级控制流劫持方案

- 3.1 进程执行的更多细节
- **3.2 面向返回地址编程**
- 3.3 全局偏置表劫持
- 3.4 虚假vtable劫持

面向返回地址编程

- 面向返回地址编程（Return-Oriented Programming，ROP）基于**栈区溢出攻击**，将返回地址设置为**代码段中的合法指令**，组合现存指令修改寄存器，劫持进程控制流

ROP利用进程内存空间当中现存的指令，**“编写”**恶意程序，劫持进程的控制流

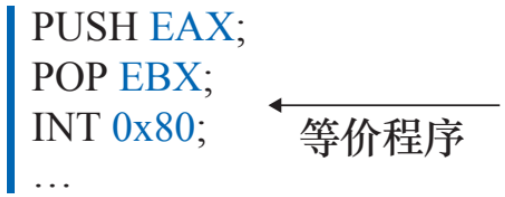


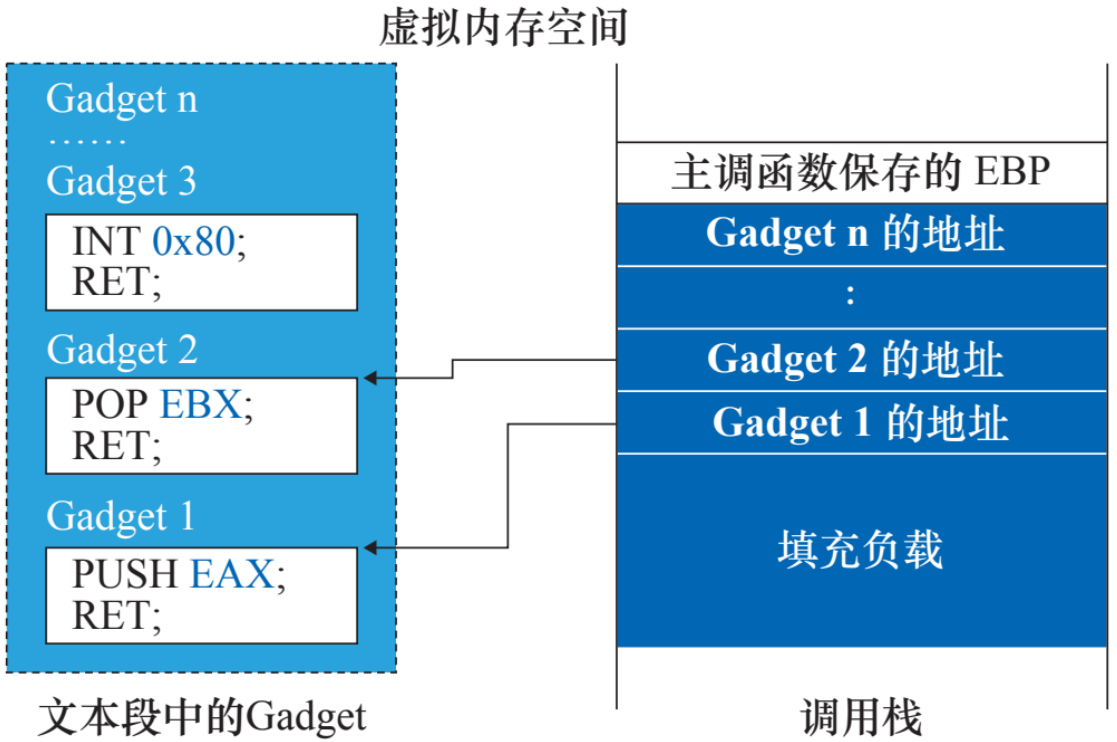
面向返回地址编程

- 面向返回地址编程构造恶意程序所需的指令片段被称为 **Gadget**

Gadget均以**RET指令**结尾

当一个Gadget执行后，**RET指令**将跳转执行下一个Gadget



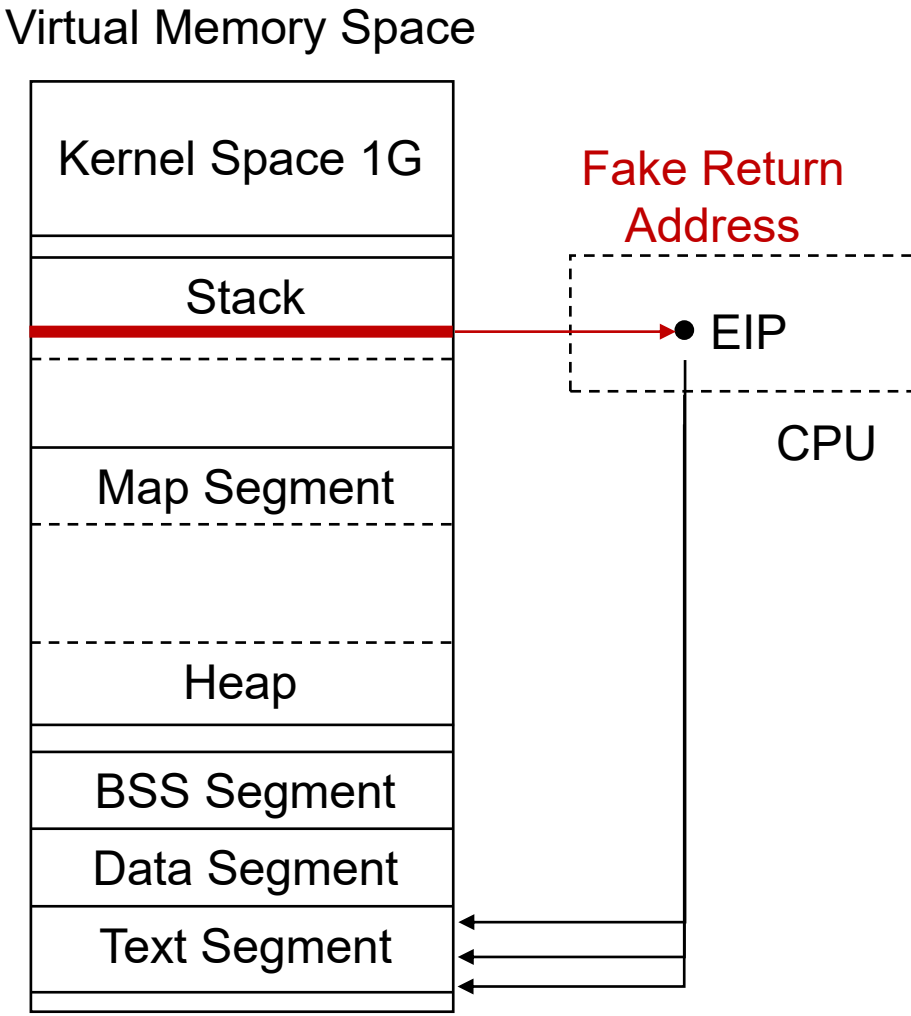


注. Gadget在代码段，地址固定，可以通过逆向工程工具直接获得

面向返回地址编程的优势

- **面向返回地址编程的优势**
- 面向返回地址编程（ROP）**可以绕过NX** 防御机制，因为虚假的返回地址被设置在代码段（Text Segment），代码段是存放进程指令的内存区域，必有执行权限

- 面向返回地址编程（ROP）**可以绕过ASLR 防御机制**，因为恶意代码并不需直接放在堆区，从而不需要确定地址。



面向返回地址编程总结

对面向返回地址编程（ROP）攻击的讨论与总结：

- ROP的本质是利用程序**代码段的合法指令**，重组一个恶意程序，每一个可利用的指令片段被称作 Gadget，可以说ROP是：a chain-of-gadgets
- ROP可以绕过NX和ASLR防御机制，但对于Stack Canary则需要额外的信息泄露方案才可绕过这一防御机制
- ROP使用的Gadget以RET指令结尾；若Gadget的结尾指令为JMP，则为**面向跳转地址编程**（Jump-Oriented Programming，JOP），原理与ROP类似

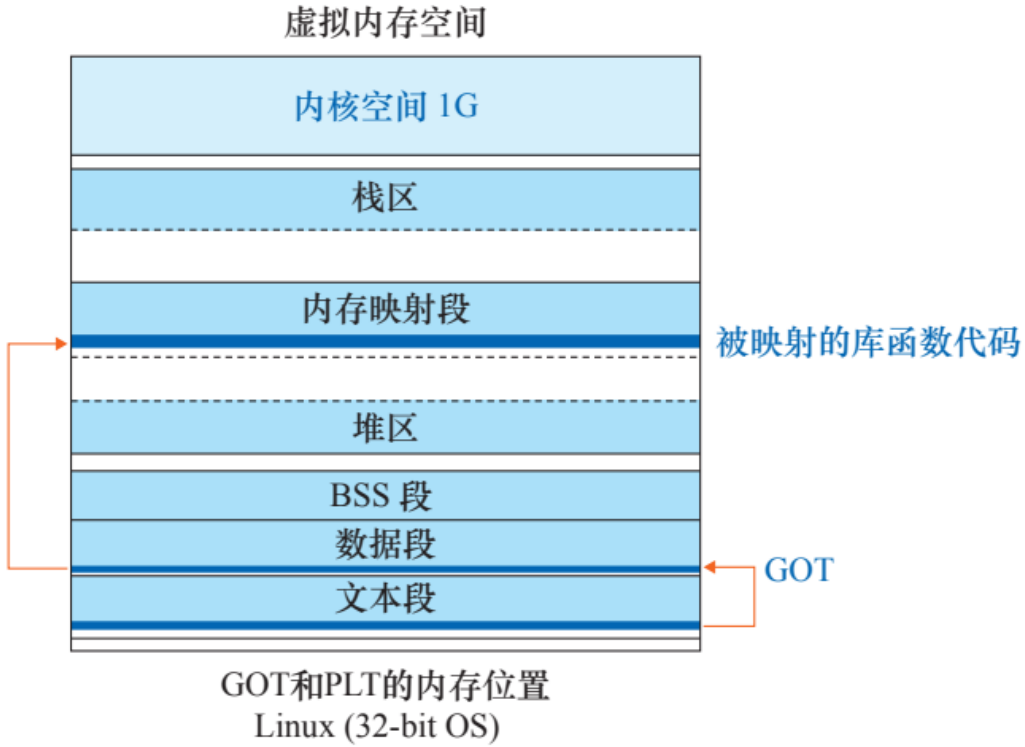
第3节 高级控制流劫持方案

- 3.1 进程执行的更多细节
- 3.2 面向返回地址编程
- **3.3 全局偏置表劫持**
- 3.4 虚假vtable劫持

全局偏移表与程序链接表

- 为了使进程可以找到内存中的动态链接库，需要维护位于**数据段**的**全局偏移表**（Global Offset Table，GOT）和位于**代码段**的**程序连接表**（Procedure Linkage Table，PLT）

- 程序使用**CALL指令**调用共享库函数；其调用地址为**PLT表地址**，而后由PLT表**跳转索引GOT表**，GOT表项指向内存映射段，也就是位于动态链接库的库函数

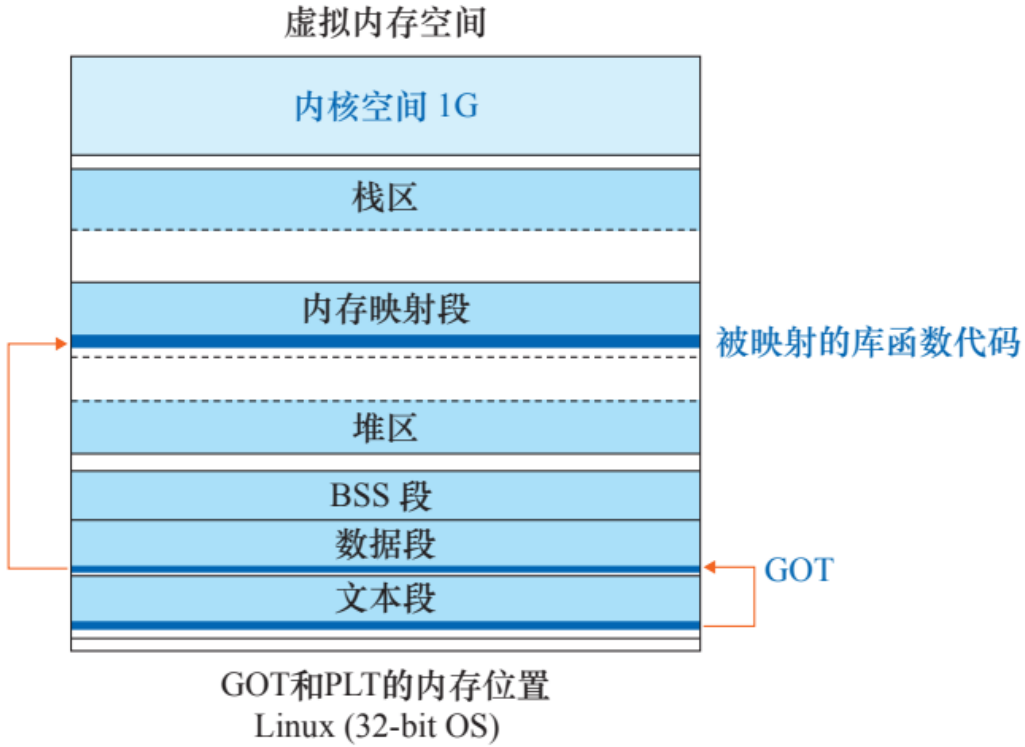


全局偏移表与程序链接表

- PLT表在运行前确定，且在程序运行过程中不可修改（Text Segment 不可写）

GOT表根据一套“惰性的”共享库函数加载机制，GOT表项在库函数的首次调用时确定，指向正确的内存映射段位置

- **动态链接器**将完成共享库在的映射，并为GOT确定表项



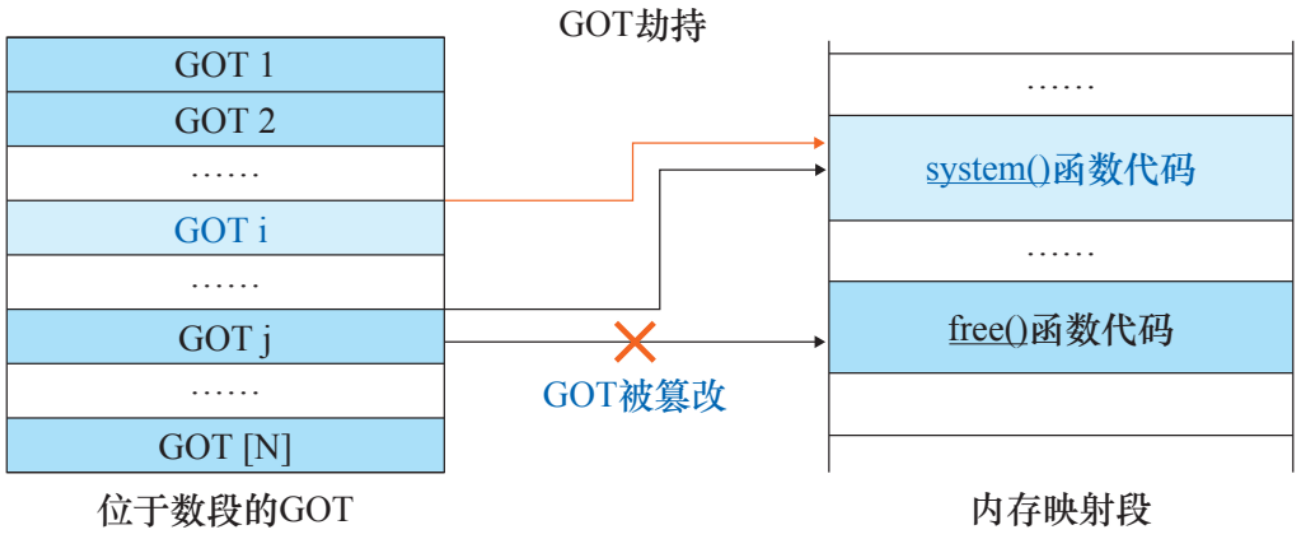
GOT和PLT的内存位置
Linux (32-bit OS)

注. 动态链接器为最早被加载的动态链接库

全局偏移表劫持

- GOT Hijacking (全局偏置表劫持)攻击的本质是恶意篡改GOT表，使进程调用攻击者指定的库函数，实现控制流劫持

如图，当GOT表被修改后，当攻击者调用free函数时，实际上将调用system函数



全局偏移表劫持的优势

- **全局偏置表劫持的优势：**

- **GOT Hijacking攻击可以绕过NX保护机制。**因为装载共享库函数的页上必须有可执行权限；且GOT表位于数据段，数据段可读可写

- **GOT Hijacking攻击可以绕过ASLR保护机制。**因为ASLR无法随机化代码段的位置，攻击者仍然可以通过PLT表恶意读取GOT表项目，而后得到动态库当中函数的地址

全局偏移表劫持步骤

- GOT Hijacking可以分为大致如下的几个步骤：

1. 攻击者通过读PLT确定要被修改的受害GOT表项的地址
2. 攻击者读取这一GOT表项，得到任一库函数的内存映射段地址
3. 攻击者将得到的地址加一个偏置，得到希望被恶意调用的函数的内存映射段地址
4. 攻击者将这一地址写入定位好的受害GOT表项当中

其中，恶意读写GOT表项既可以通过基于栈溢出的ROP来实现，也可以通过基于堆溢出的任意位置读写来实现

全局偏移表劫持总结

- **GOT Hijacking的总结：**
- GOT Hijacking本质上是一种修改GOT表项来实现的控制流劫持；这种攻击方案要依赖于栈区溢出等基础攻击方式才可以实现
- 这种攻击方案可以绕过NX与ASLR防御机制
- 目前已有RELRO（read only relocation）机制，可将GOT表项映射到只读区域上，一定程度上预防了对GOT表的攻击

第3节 高级控制流劫持方案

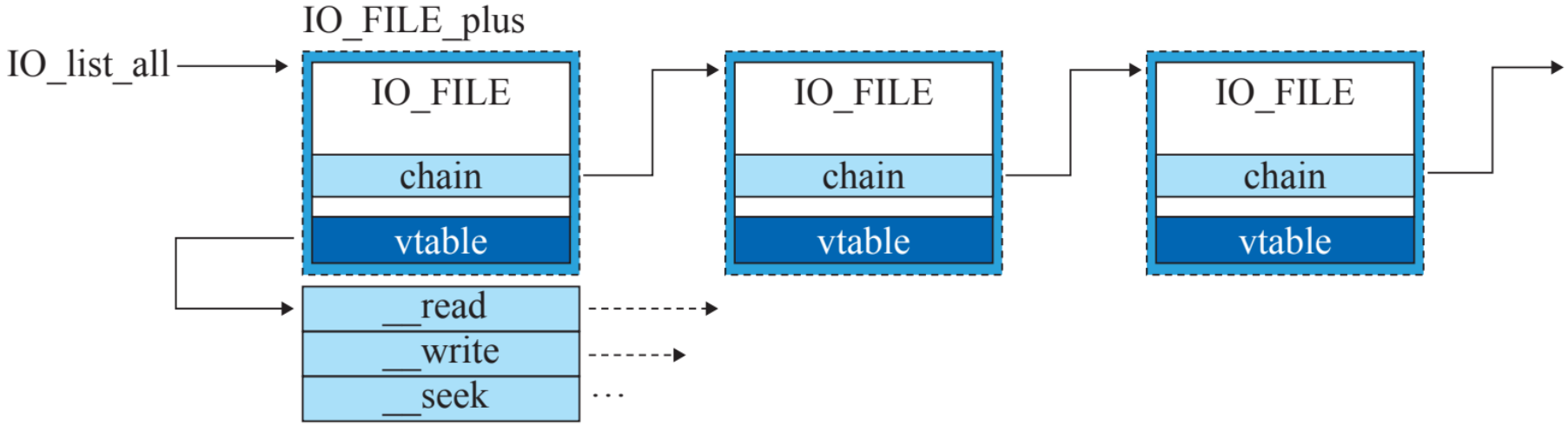
- 3.1 进程执行的更多细节
- 3.2 面向返回地址编程
- 3.3 全局偏置表劫持
- **3.4 虚假vtable劫持**

文件系统角度的安全威胁

- **Linux文件系统维护的元数据：**

在 Linux 系统的标准文件I/O库中 IO_FILE 结构用于描述文件；该结构在程序执行 fopen 等函数时会进行创建，并**分配在堆区**中

IO_FILE 结构外层包裹 IO_FILE_plus 结构，并会通过 chain 字段彼此连接形成一个链表，链表头部用全局变量 IO_list_all 表示



针对文件系统攻击的本质是：恶意操纵文件系统的管理数据结构

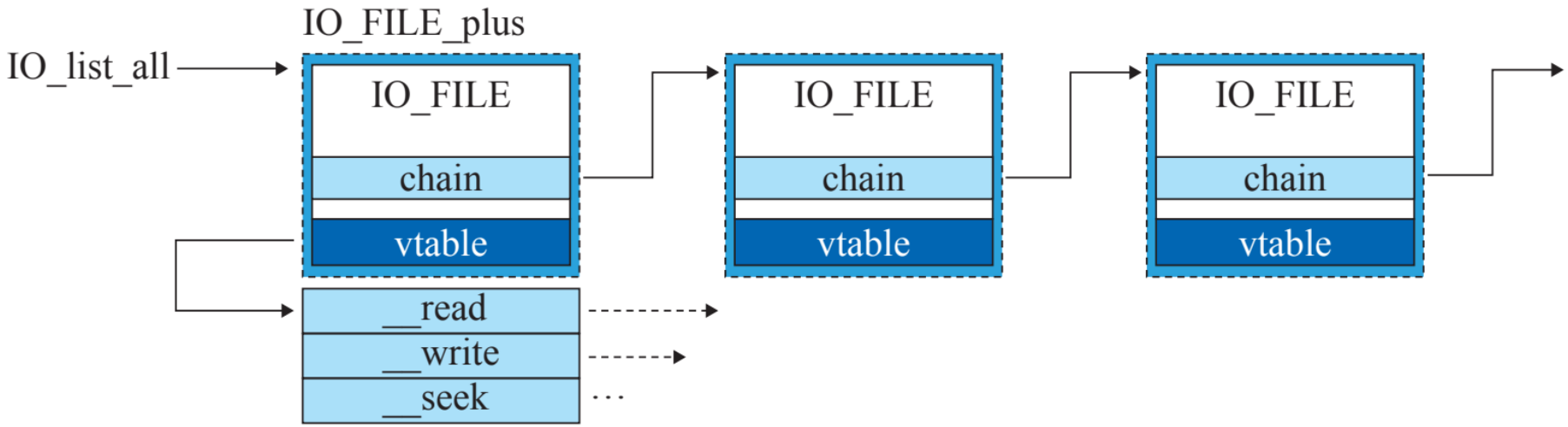
虚假vtable劫持攻击

- **虚假vtable劫持攻击 （Fake vtable Hijacking）**

Linux 中的文件 I/O 操作函数都需要经过 IO_FILE 结构进行处理，尤其是结构中的**vtable**字段，大部分函数会取出vtable指向的一系列**基础文件操作函数**进行调用

虚假vtable劫持攻击的核心是：篡改文件管理数据结构中的vtable字段

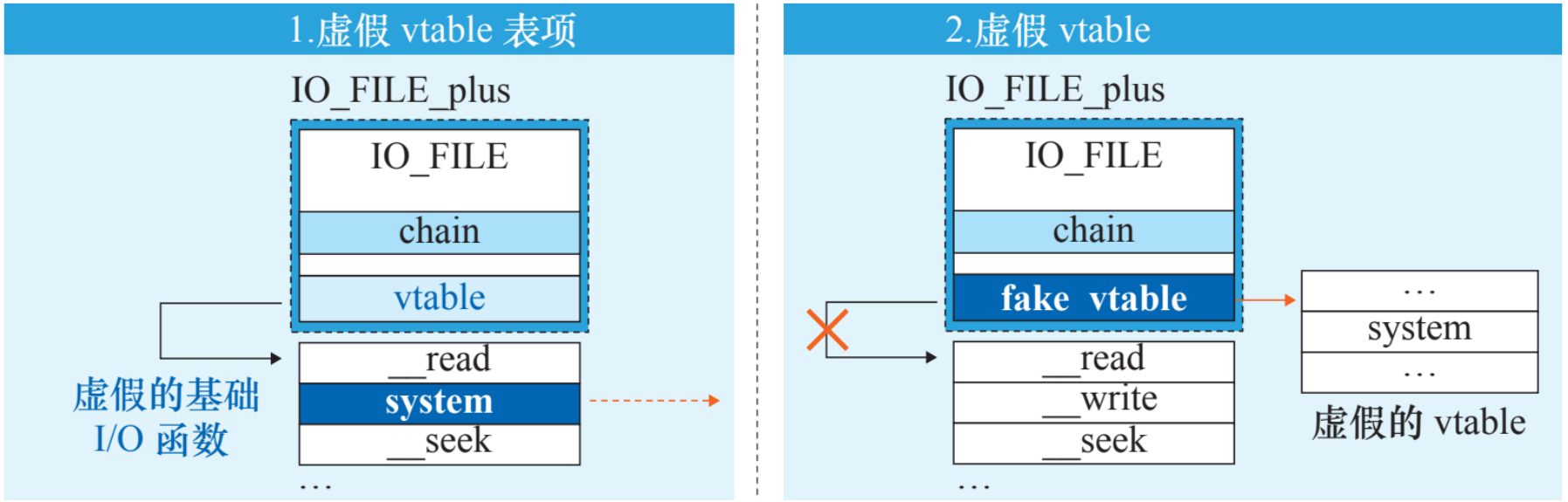
通过把vtable指向攻击者控制的内存，并在其中布置函数指针



虚假vtable劫持攻击

- **虚假vtable劫持攻击，2种具体实现：**

1. 直接改写vtable指向的函数指针，可通过构造**堆块覆盖**完成
2. 覆盖vtable字段，使其指向攻击者控制的内存，然后在其中布置函数指针



第4节 高级操作系统保护方案

- **4.1 控制流完整性保护**
- 4.2 指针完整性保护
- 4.3 信息流控制
- 4.4 I/O子系统保护

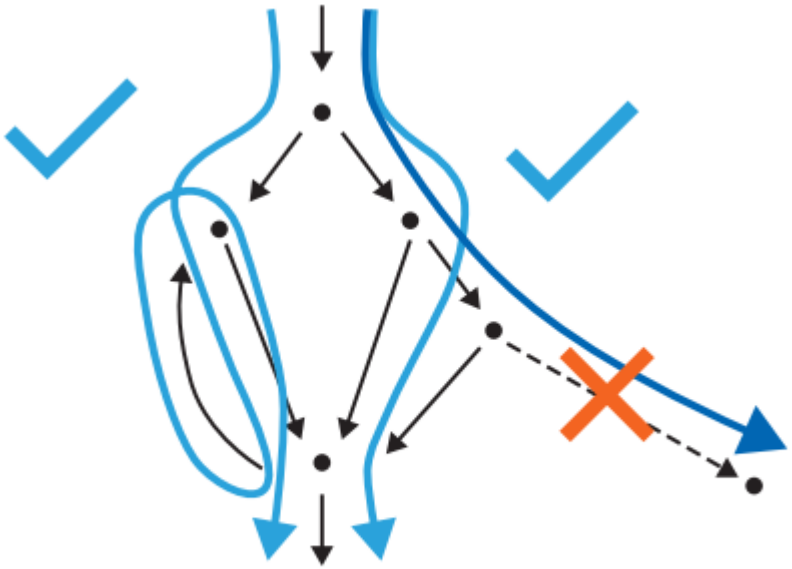
控制流完整性保护

- 控制流完整性保护（CFI）防御机制的核心思想是限制程序运行中的控制流转移，使其始终处于原有的控制流图所限定的范围

- 主要分为两个阶段：

1. 通过二进制或者源代码程序分析得到控制流图(CFG)，获取转移指令目标地址的列表

2. 运行时检验转移指令的目标地址是否与列表中的地址相对应；控制流劫持会违背原有的控制流图，CFI 则可以检验并阻止这种行为



控制流图

第4节 高级操作系统保护方案

- 4.1 控制流完整性保护
- **4.2 指针完整性保护**
- 4.3 信息流控制
- 4.4 I/O子系统保护

指针完整性保护

- **拓展性内容：指针完整性保护CPI**

Volodymyr K, Laszlo S, et al. Code-pointer integrity. OSDI 2014.

与CFI提出动机相同：CPI的提出动机仍然是因为ASLR和DEP等内存保护无法防御ROP等进程控制流劫持方案

CPI希望解决CFI的高开销问题，其核心在于控制和约束指针的指向位置

关于CPI**是否可用**的性能评价性研究请参考脚注[1]

1. Isaac Evans, et al. "Missing the point (er): On the effectiveness of code pointer integrity." 2015 IEEE Symposium on Security and Privacy. IEEE, 2015.

第4节 高级操作系统保护方案

- 4.1 控制流完整性保护
- 4.2 指针完整性保护
- **4.3 信息流控制**
- 4.4 I/O子系统保护

信息流控制

- **信息流控制**，Information Flow Control（IFC）是一种操作系统**访问权限控制方案（Access Control）**

操作系统可以利用IFC控制进程访问数据的能力[1]
分布式操作系统可以使用IFC控制节点间信息交换的能力[2]

- 即便程控制流被劫持，IFC可以保证受害进程无法具备正常执行之外的能力；例如，访问文件系统中的密钥对，调用操作系统的网络服务

1. Nickolai Zeldovich, et al. "Making information flow explicit in HiStar." In Proc. of the 7th OSDI, 2006.
2. Nickolai Zeldovich, et al. "Securing Distributed Systems with Information Flow Control. " In NSDI 2008.

信息流控制

- **信息流控制的三要素：**

1. 约束：调用服务或访问数据需要满足什么样的要求，需要有什么权限才可访问
   > IFC中以Label的形式体现
2. 权限：标志进程具有哪些被赋予的权限，IFC中权限可以动态获取
   > IFC中以Ownership[1] 的形式体现
3. 属性：权限和约束当中包含的单元，是访问能力的元数据形式
   > IFC中以Categories的形式体现

信息流可流动的条件是：
进程的**权限**满足**约束**对其中全部**属性**的要求

1. 部分文献亦称之为privilege，与Ownership完全等价

第4节 高级操作系统保护方案

- 4.1 控制流完整性保护
- 4.2 指针完整性保护
- 4.3 信息流控制
- **4.4 I/O子系统保护**

I/O 子系统保护

I/O 子系统是操作系统的重要组成部分

- I/O 子系统是操作系统一个**重要而庞大**的模块，实现了网络协议栈与一系列复杂的人机交互功能；有文献证实，Linux 中I/O子系统占据了超过**70%**的代码量

- 在内核当中实现有USB (Universal Serial Bus)，蓝牙 (BlueTooth) 等一系列外设I/O交互协议；
- 也包含了完整的网络协议栈，例如TCP/IP协议栈：IPv4/6，ICMP，TCP，UDP等一系列协议

针对I/O子系统的攻击的本质是：发掘通讯协议中的漏洞

I/O 子系统保护

针对网络 I/O 的攻击与保护方案

- 需要时刻牢记，**内核协议栈是操作系统的组成部分之一**，因而面向网络当中端节点的攻击方案的本质均是面向**操作系统网络I/O子系统**的攻击

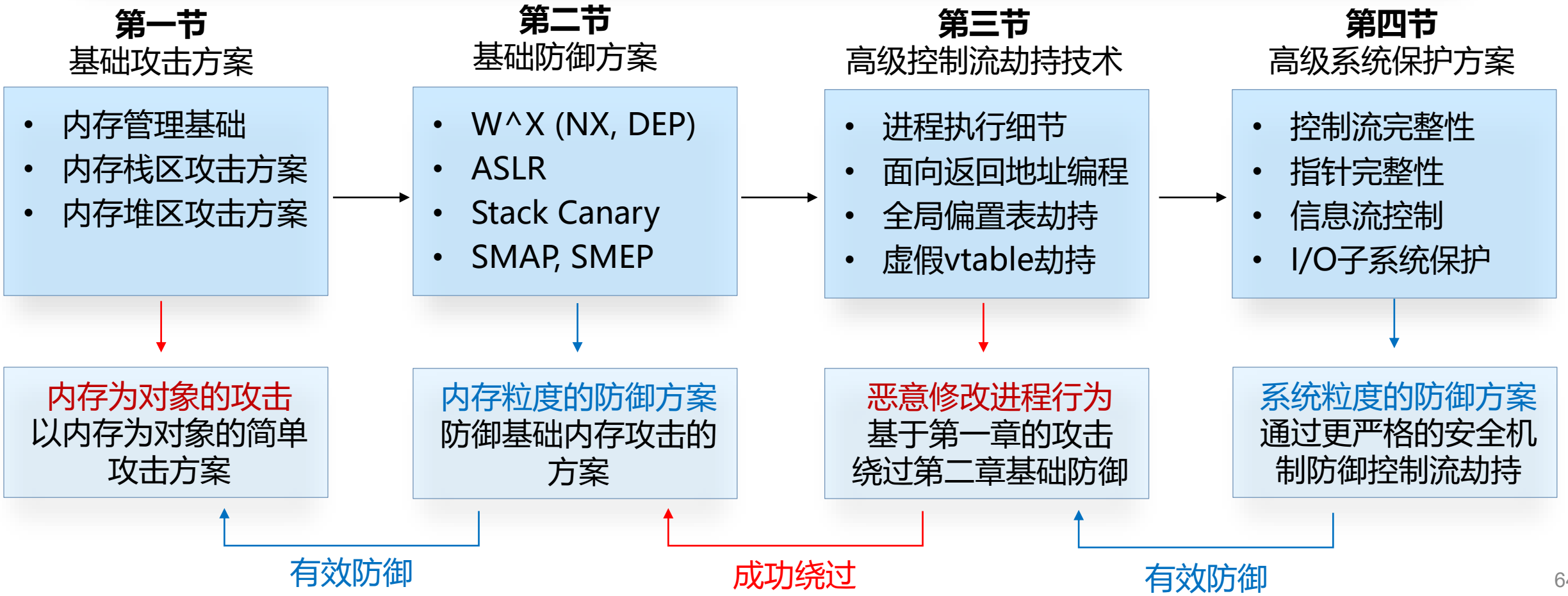
- 例如，TCP侧信道攻击发掘内核协议栈当中的设计或者实现上的缺陷，是对操作系统网络I/O的攻击方案，需要借助**网络入侵检测系统**进行保护

- **关于网络协议栈的攻击/保护方案，将在第八章详细展开**

第5节 总结和展望

总结

本章当中，我们首先回顾了最早的操作系统安全问题，Morris Worm；并分析了 SQL Slammers 侵染SQL Server的全过程，之后由浅入深地介绍了操作系统下一系列攻击与防御方案



展望

宏观来看操作系统安全研究发展趋势有二：

- 其一，对于操作系统的防御与攻击方案**与新型硬件特性**加以结合，例如：

Gras, et al.[1] 在2017年提出了一种利用硬件缓存侧信道去除ASLR随机化的方法

Frassetto, et al.[2] 通过拓展指令集，实现了内存隔离，防止了非法内存访问的发生

借助SGX，MPK等新型硬件安全功能，借助硬件虚拟化基础设施实现新的系统安全保障机制研究目前是一个**活跃的研究分支**

1. Ben Gras, et al. "ASLR on the Line: Practical Cache Attacks on the MMU." NDSS. Vol. 17. 2017.
2. Tommaso Frassetto, et al. "IMIX: In-Process Memory Isolation EXtension." 27th USENIX Security Symposium, 2018.

展望

宏观来看操作系统安全研究发展趋势有二：

- 其二，操作系统环境下的**漏洞的自动化挖掘**

Wang, et al.[1] 实现了一种对于操作系统缺乏二次检查漏洞的全自动化挖掘方法，其使用的传统数据流与控制流分析，类似的工作还有很多

Jia, et al.[2] 针对于内核驱动当中的未初始化漏洞进行了分析

Eckert, et al.[3] 利用模型验证（Model Checking）方法实现了对于堆管理器的安全性验证

1. Wenwen Wang, et al. “Check it again: Detecting lacking-recheck bugs in os kernels." in Proceedings of CCS, 2018.
2. Xiangkun Jia, et al. "Towards efficient heap overflow discovery." 26th USENIX Security Symposium, 2017.
3. Moritz Eckert, et al. "Heaphopper: Bringing bounded model checking to heap implementation security." 27th USENIX Security Symposium, 2018.

展望

宏观来看操作系统安全研究发展趋势有二：

- 其二，操作系统**漏洞的自动化挖掘**

目前系统相关漏洞自动化挖掘是极其活跃的研究分支

然而，其中具有显著成效的方法均以传统的**静态源代码分析**为主，具有更好漏洞挖掘效果的**动态分析方案**（例如模糊测试，Fuzzing）在应用到操作系统这类高度复杂软件系统时仍然存在各种各样的局限性

目前来看，精准全面的操纵系统漏洞的自动化挖掘仍然是一个“美好的理想”