Play with FILE Structure

Yet Another Binary Exploit Technique

Angelboy

Agenda

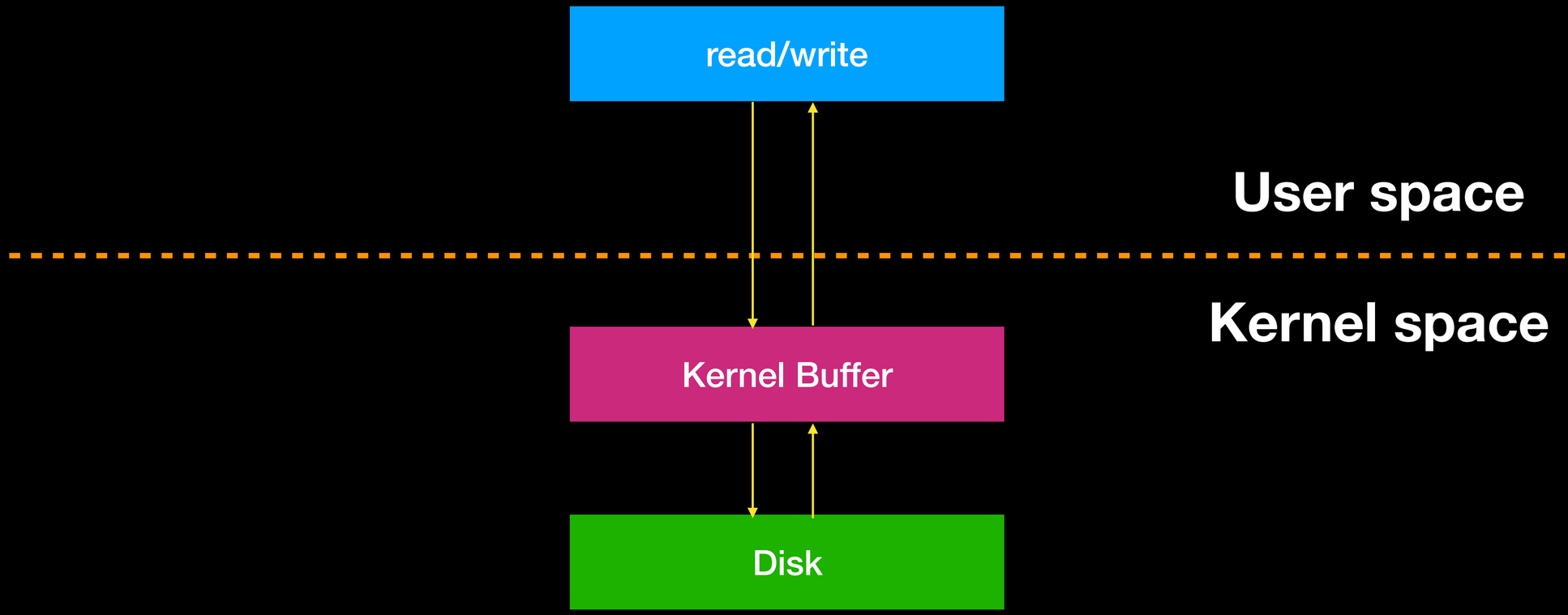
- Introduction
  - File stream
  - Overview the FILE structure
- Exploitation of FILE structure
  - FSOP
  - Vtable verification in FILE structure
  - Make FILE structure great again
- Conclusion

Agenda

- Introduction
  - File stream
  - Overview the FILE structure
- Exploitation of FILE structure
  - FSOP
  - Vtable verification in FILE structure
  - Make FILE structure great again
- Conclusion

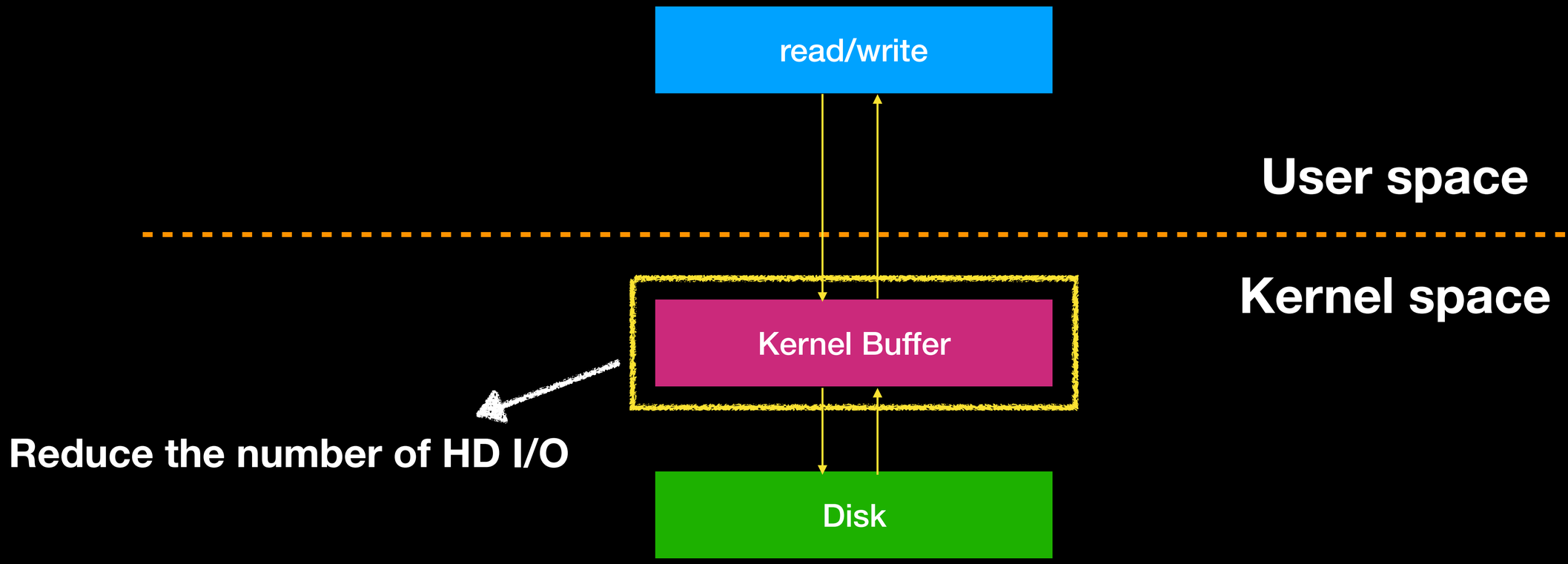
Introduction

- What happen when we use a raw IO function



Introduction

- What happen when we use a raw IO function

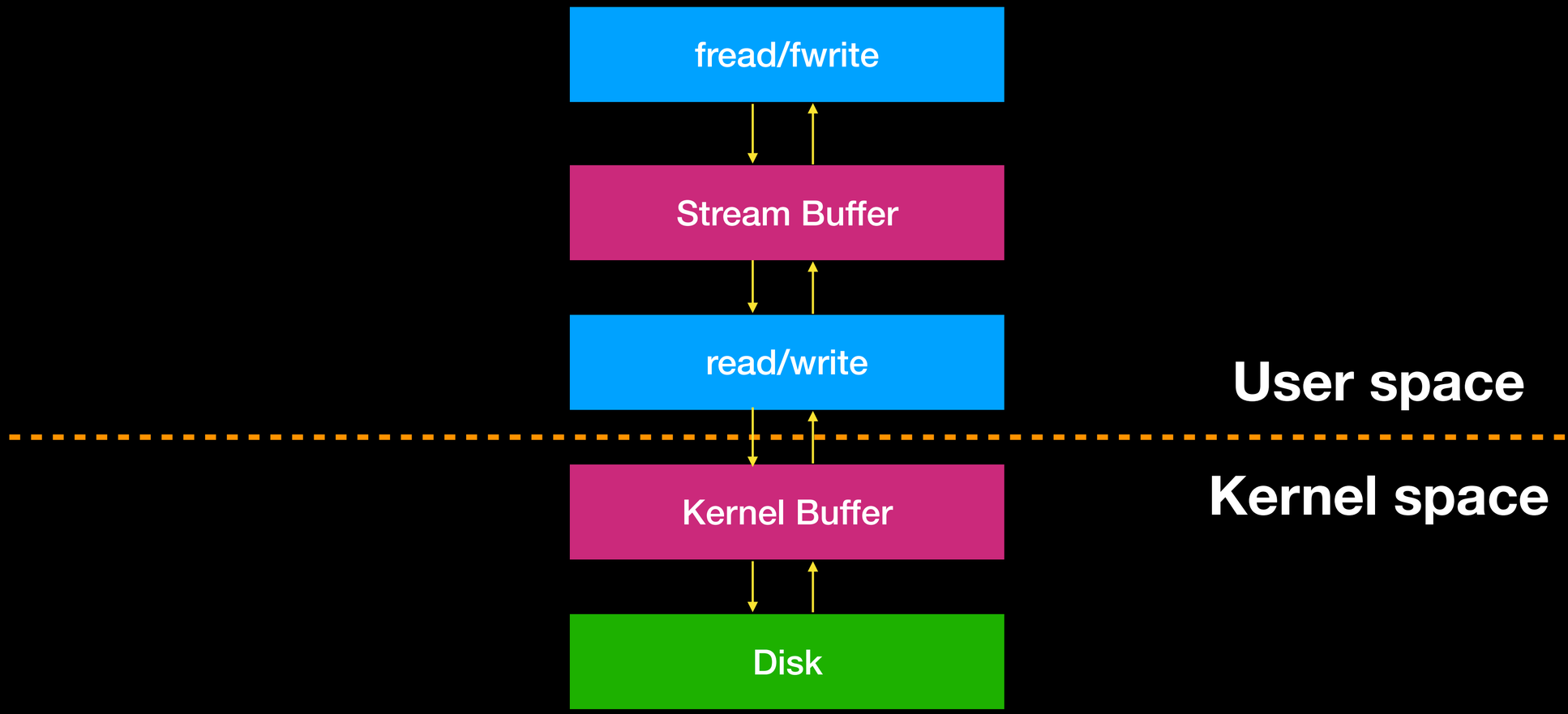


Introduction

- What is File stream
  - A higher-level interface on the primitive file descriptor facilities
  - Stream buffering
  - Portable and High performance
- What is FILE structure
  - A File stream descriptor
  - Created by fopen

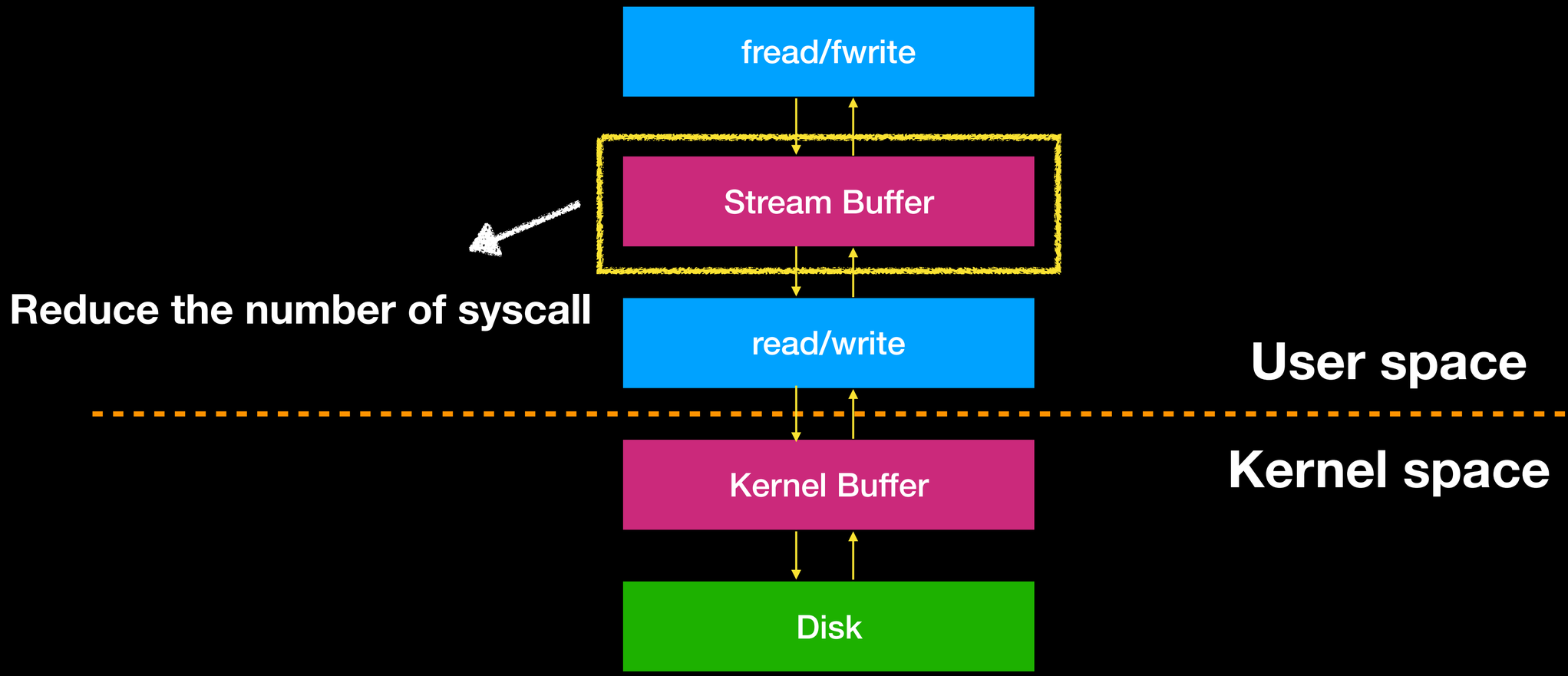
Introduction

- What happen when we use **stdio function**



Introduction

- What happen when we use **stdio function**



Agenda

- Introduction
  - File stream
  - Overview the FILE structure
- Exploitation of FILE structure
  - FSOP
  - Vtable verification in FILE structure
  - Make FILE structure great again
- Conclusion

Introduction

- FILE structure
  - A complex structure
    - Flags
    - Stream buffer
    - File descriptor
  - FILE_plus
    - Virtual function table

```
struct _IO_FILE {
  int _flags;   /* High-order w
#define _IO_file_flags _flags

  /* The following pointers co
  /* Note:  Tk uses the _IO_rea
  char* _IO_read_ptr; /* Curren
  char* _IO_read_end; /* End of
  char* _IO_read_base;  /* Star
  char* _IO_write_base; /* Star
  char* _IO_write_ptr;  /* Curr
  char* _IO_write_end;  /* End
  char* _IO_buf_base; /* Start
  char* _IO_buf_end;  /* End of
  /* The following fields are u
  char *_IO_save_base; /* Point
  char *_IO_backup_base;  /* Po
  char *_IO_save_end; /* Pointe

  struct _IO_marker *_markers;

  struct _IO_FILE *_chain;

  int _fileno;
```

Introduction

- FILE structure
  - Flags
    - Record the attribute of the File stream
      - Read only
      - Append
      - ...

```
struct _IO_FILE {
  int _flags;   /* High-order
#define _IO_file_flags _flags

  /* The following pointers co
  /* Note:  Tk uses the _IO_rea
  char* _IO_read_ptr; /* Curre
  char* _IO_read_end; /* End o
  char* _IO_read_base;  /* Sta
  char* _IO_write_base; /* Sta
  char* _IO_write_ptr;  /* Cur
  char* _IO_write_end;  /* End
  char* _IO_buf_base; /* Start
  char* _IO_buf_end;  /* End o
  /* The following fields are
  char *_IO_save_base; /* Poin
  char *_IO_backup_base;  /* P
  char *_IO_save_end; /* Pointe

  struct _IO_marker *_markers;

  struct _IO_FILE *_chain;

  int _fileno;
```

Introduction

- FILE structure
  - Stream buffer
    - Read buffer
    - Write buffer
    - Reserve buffer

```
struct _IO_FILE {
  int _flags;   /* High-order w
#define _IO_file_flags _flags

  /* The following pointers co
  /* Note:  It uses the _IO_re
  char* _IO_read_ptr; /* Curre
  char* _IO_read_end; /* End o
  char* _IO_read_base;  /* Sta
  char* _IO_write_base; /* Sta
  char* _IO_write_ptr;  /* Cur
  char* _IO_write_end;  /* End
  char* _IO_buf_base; /* Start
  char* _IO_buf_end;  /* End o
  /* The following fields are
  char *_IO_save_base; /* Poin
  char *_IO_backup_base;  /* P
  char *_IO_save_end; /* Pointe

  struct _IO_marker *_markers;

  struct _IO_FILE *_chain;

  int _fileno;
```

Introduction

- FILE structure
  - _fileno
    - File descriptor
    - Return by sys_open

```
struct _IO_FILE {
  int _flags;   /* High-order v
#define _IO_file_flags _flags

  /* The following pointers co
  /* Note:  Tk uses the _IO_rea
  char* _IO_read_ptr; /* Curren
  char* _IO_read_end; /* End of
  char* _IO_read_base;  /* Star
  char* _IO_write_base; /* Star
  char* _IO_write_ptr;  /* Curr
  char* _IO_write_end;  /* End
  char* _IO_buf_base; /* Start
  char* _IO_buf_end;  /* End of
  /* The following fields are
  char *_IO_save_base; /* Point
  char *_IO_backup_base;  /* Po
  char *_IO_save_end; /* Pointe

  struct _IO_marker *_markers;

  struct _IO_FILE *_chain;

  int _fileno;
```

Introduction

- FILE structure
  - FILE plus
    - stdin/stdout/stderr
    - fopen also use it
    - Extra Virtual function table
      - Any operation on file is via vtable

```
struct _IO_FILE_plus
{
  _IO_FILE file;
  const struct _IO_jump_t *vtable;
};
```

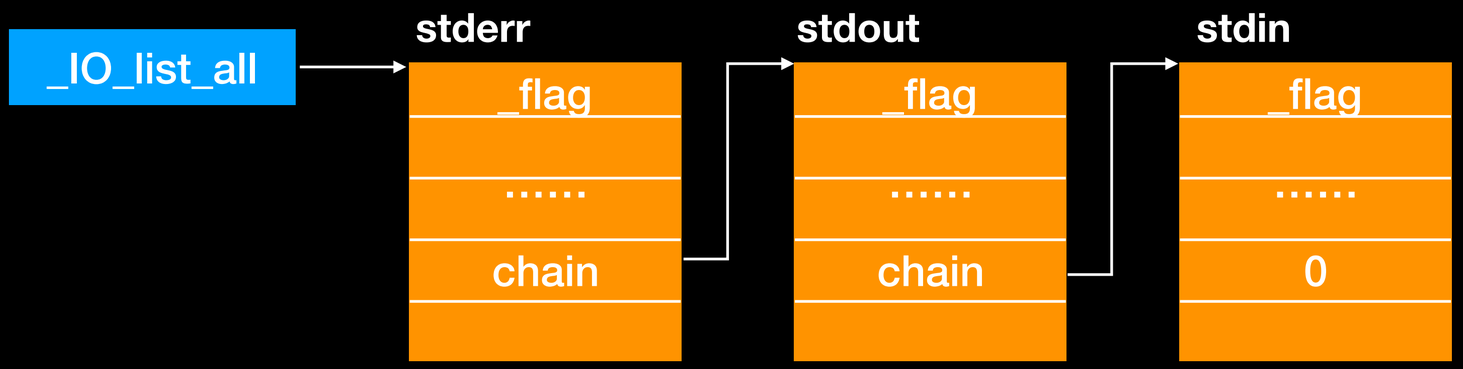
Introduction

- FILE structure
  - FILE plus
    - stdin/stdout/stderr
    - fopen also use it
    - Extra Virtual function table
      - Any operation on file is via vtable

```
const struct _IO_jump_t _IO_file_jumps libio_vtable =
{
  JUMP_INIT_DUMMY,
  JUMP_INIT(finish, _IO_file_finish),
  JUMP_INIT(overflow, _IO_file_overflow),
  JUMP_INIT(underflow, _IO_file_underflow),
  JUMP_INIT(uflow, _IO_default_uflow),
  JUMP_INIT(pbackfail, _IO_default_pbackfail),
  JUMP_INIT(xsputn, _IO_file_xsputn),
  JUMP_INIT(xsgetn, _IO_file_xsgetn),
  JUMP_INIT(seekoff, _IO_new_file_seekoff),
  JUMP_INIT(seekpos, _IO_default_seekpos),
  JUMP_INIT(setbuf, _IO_new_file_setbuf),
  JUMP_INIT(sync, _IO_new_file_sync),
  JUMP_INIT(doallocate, _IO_file_doallocate),
  JUMP_INIT(read, _IO_file_read),
  JUMP_INIT(write, _IO_new_file_write),
  JUMP_INIT(seek, _IO_file_seek),
  JUMP_INIT(close, _IO_file_close),
  JUMP_INIT(stat, _IO_file_stat),
  JUMP_INIT(showmanyc, _IO_default_showmanyc),
  JUMP_INIT(imbue, _IO_default_imbue)
};
libc_hidden_data_def (_IO_file_jumps)
```

Introduction

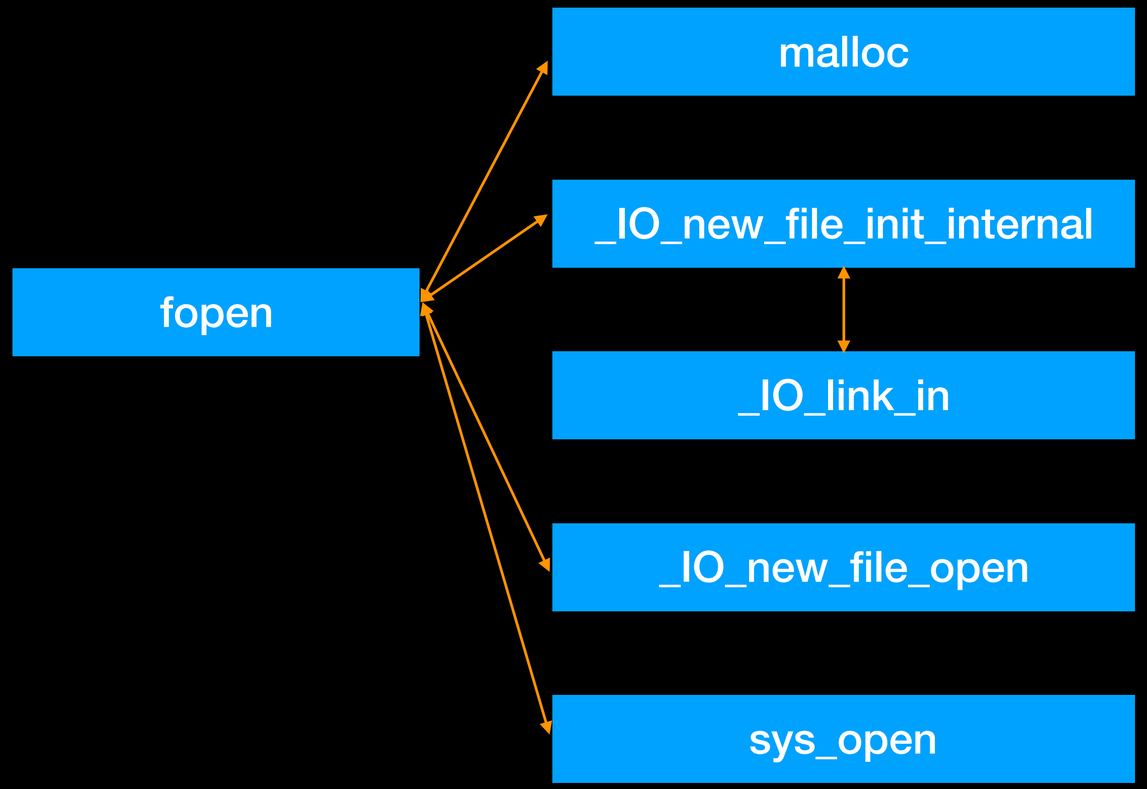
- FILE structure
  - Every FILE associate with a _chain (linked list)




```
struct _IO_FILE {
  int _flags;   /* High-order w
#define _IO_file_flags _flags

  /* The following pointers co
  /* Note:  Tk uses the _IO_rea
  char* _IO_read_ptr; /* Curren
  char* _IO_read_end; /* End of
  char* _IO_read_base;  /* Star
  char* _IO_write_base; /* Star
  char* _IO_write_ptr;  /* Curr
  char* _IO_write_end;  /* End
  char* _IO_buf_base; /* Start
  char* _IO_buf_end;  /* End of
  /* The following fields are u
  char *_IO_save_base; /* Point
  char *_IO_backup_base;  /* Po
  char *_IO_save_end; /* Pointe

  struct _IO_marker *_markers;

  struct _IO_FILE *_chain;

  int _fileno;
```

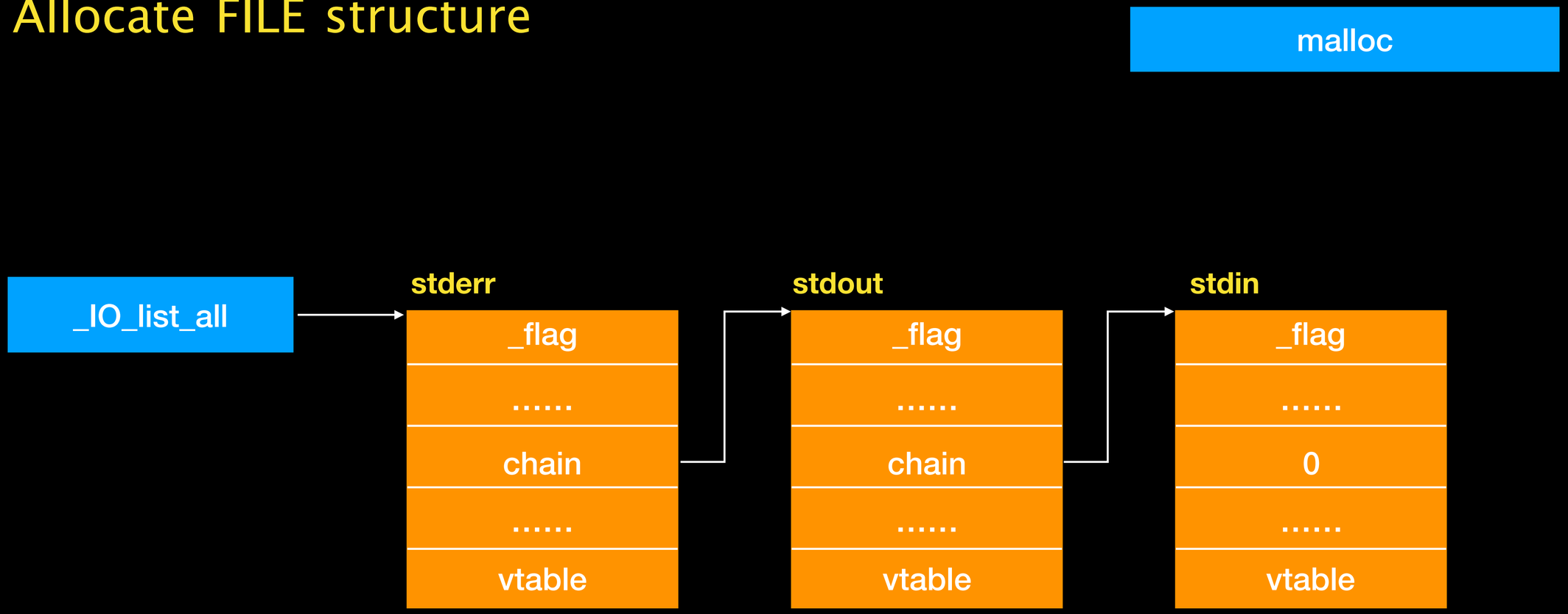
Introduction

- fopen workflow
  - Allocate FILE structure
  - Initial the FILE structure
    - Link the FILE structure
  - open file



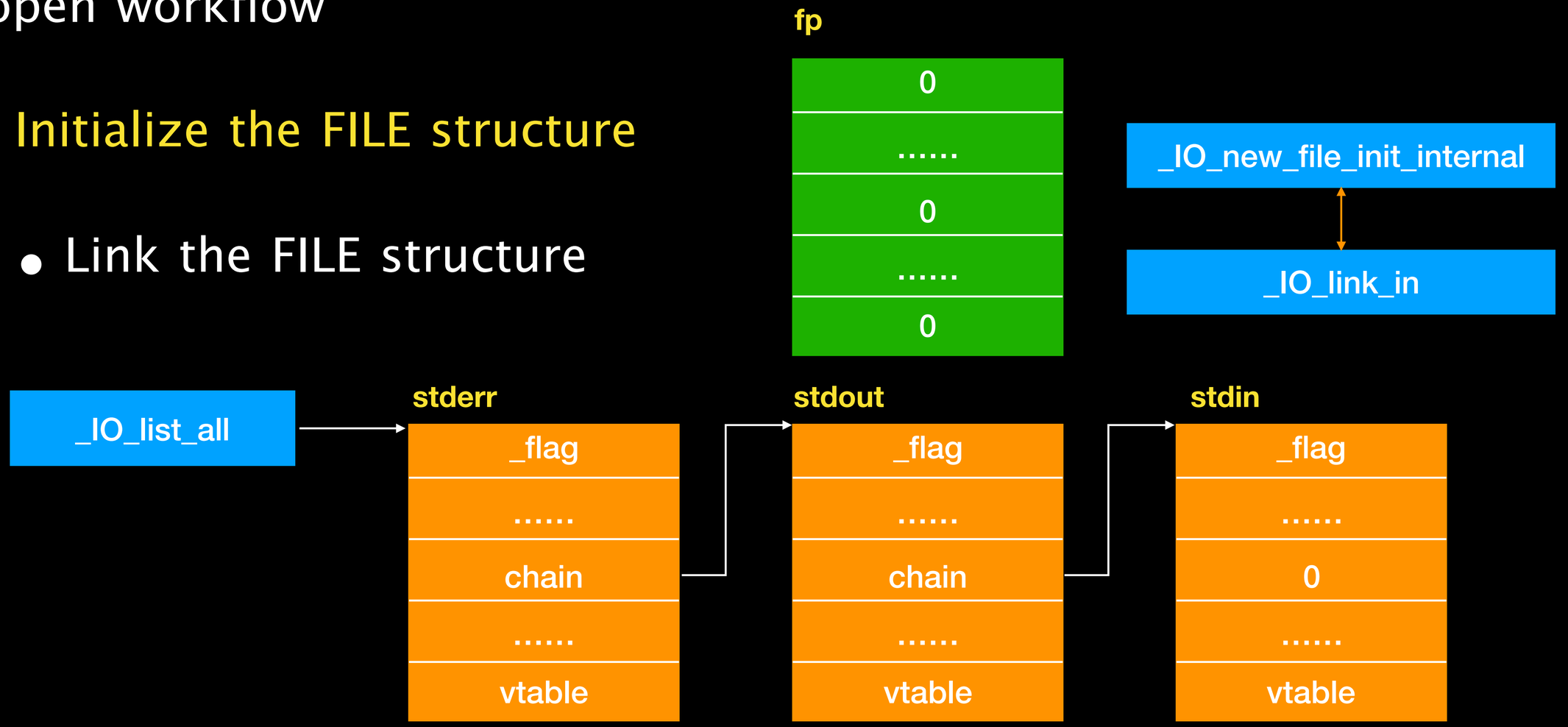
Introduction

- fopen workflow
  - Allocate FILE structure



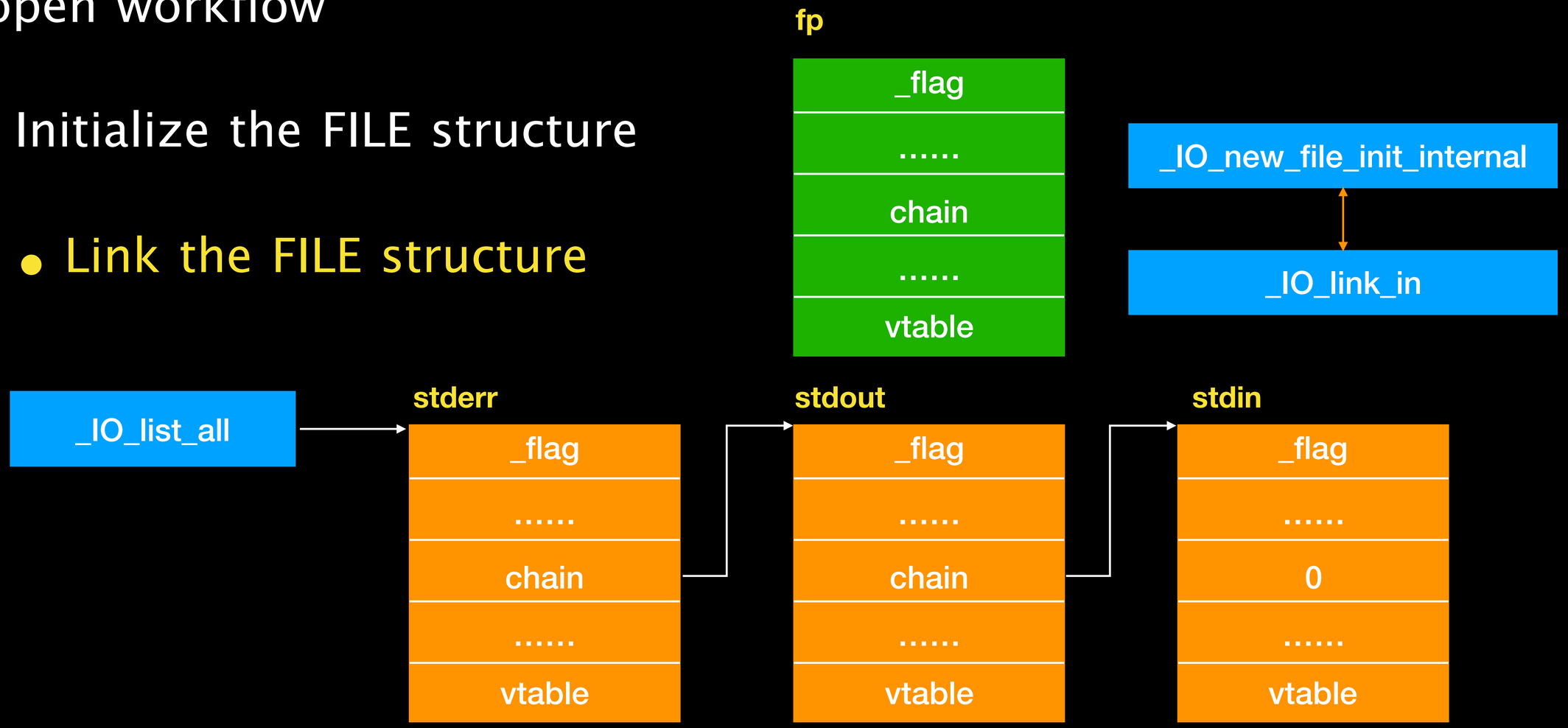
Introduction

- fopen workflow
  - Initialize the FILE structure
    - Link the FILE structure



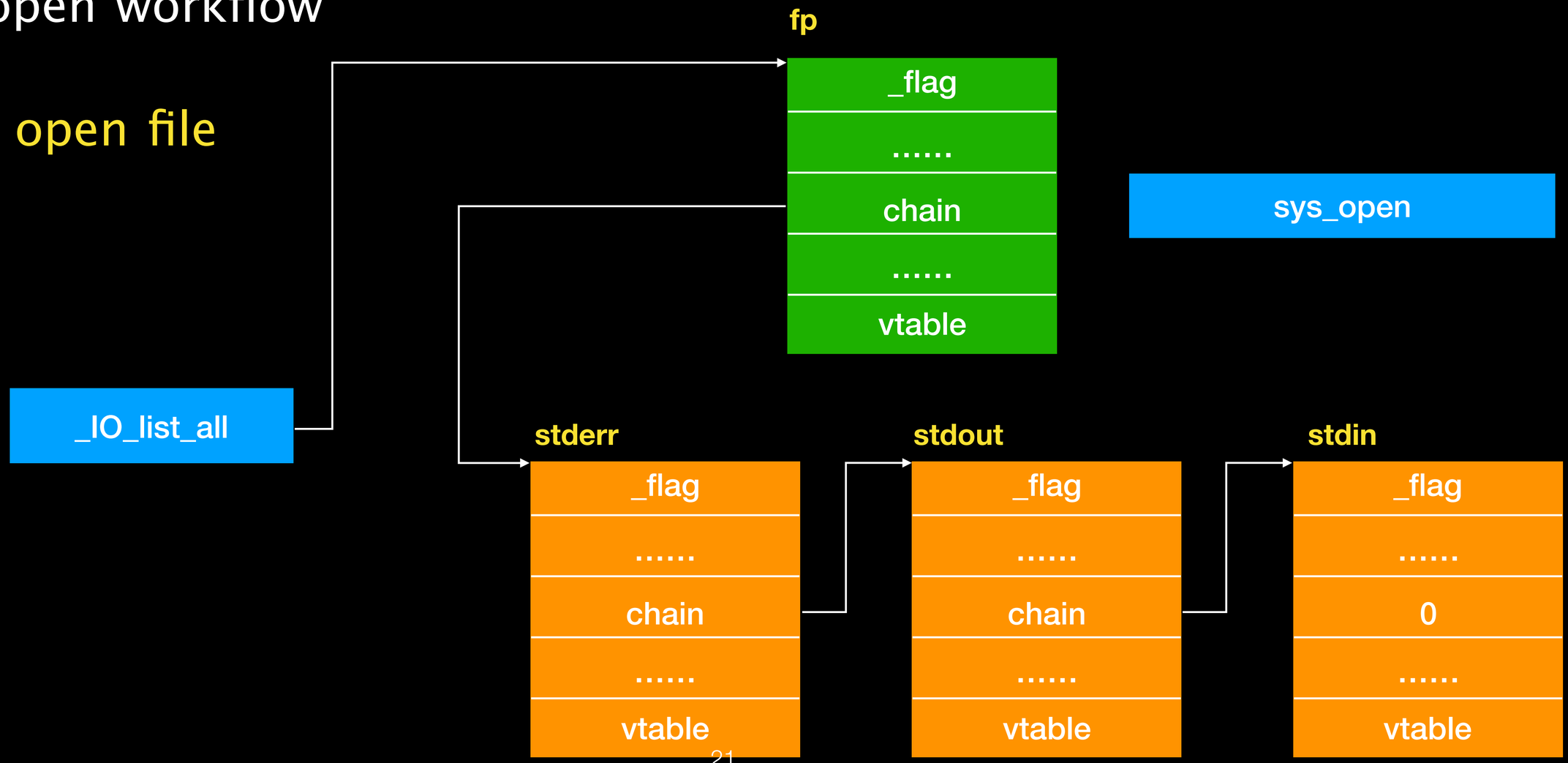
Introduction

- fopen workflow
  - Initialize the FILE structure
    - Link the FILE structure



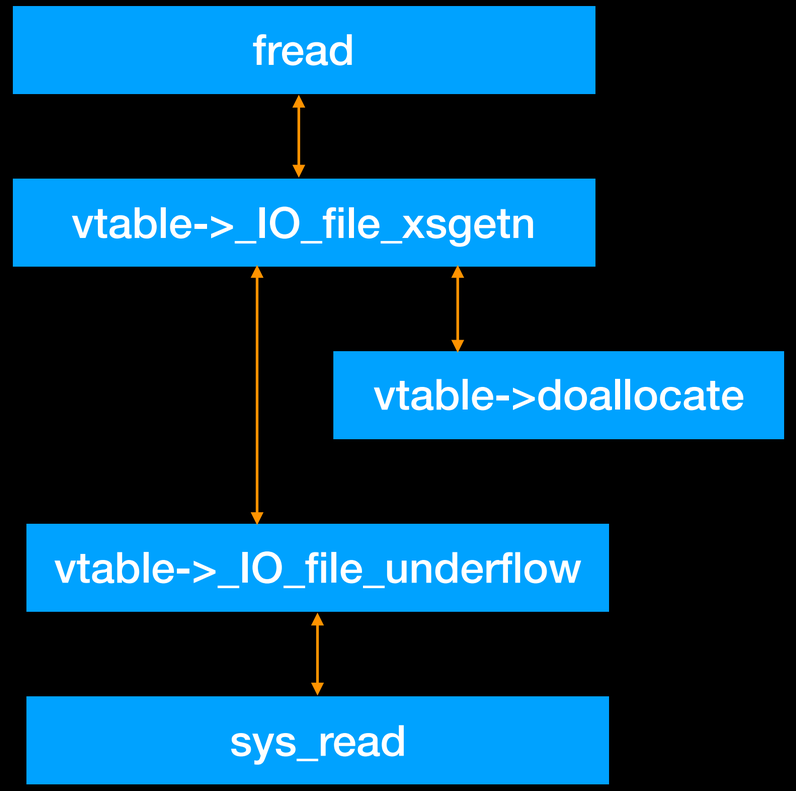
Introduction

- fopen workflow
  - open file



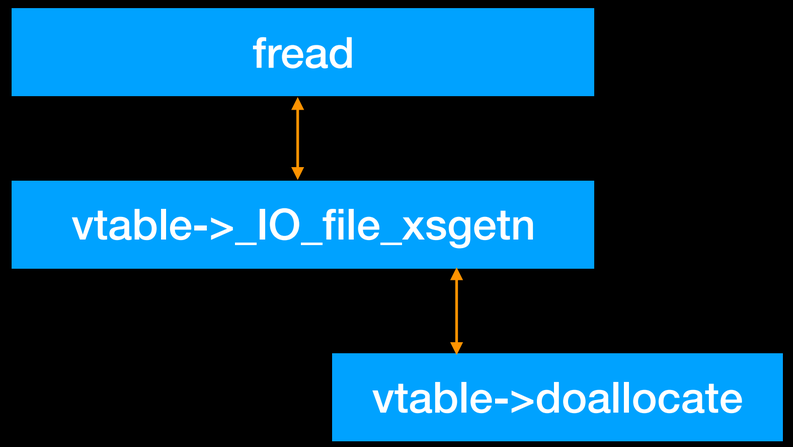
Introduction

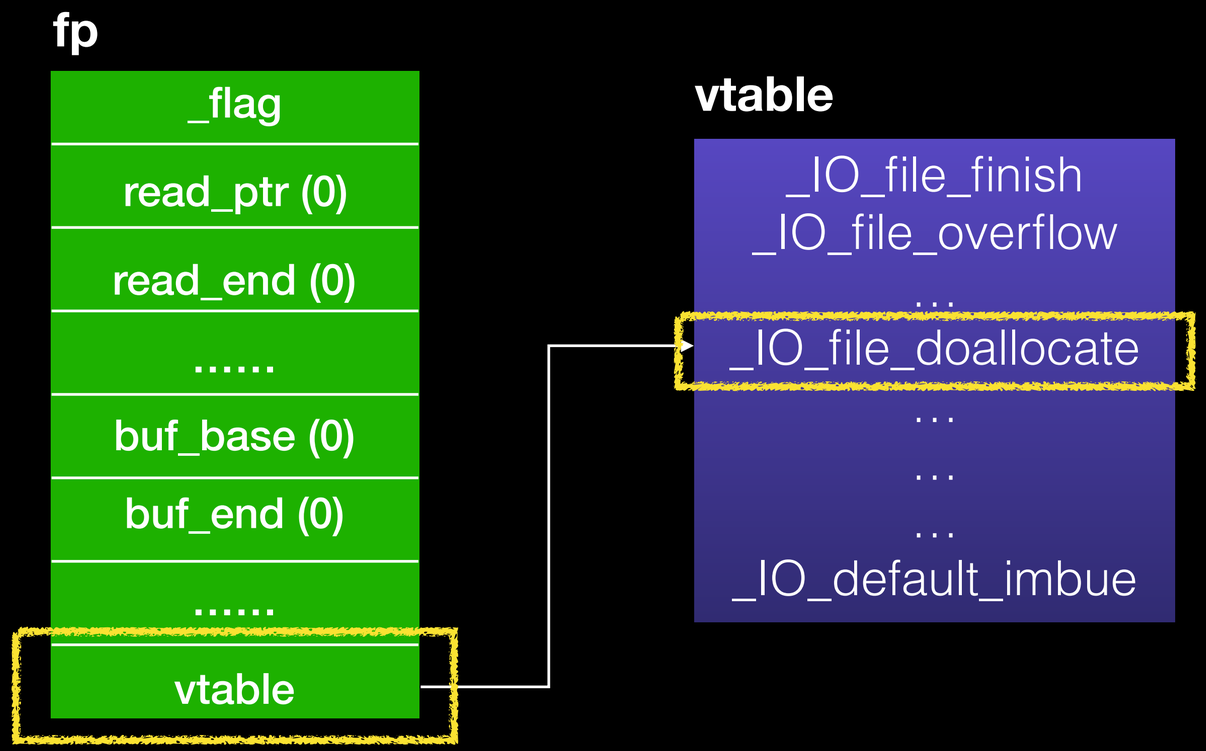
- fread workflow
  - If stream buffer is NULL
    - Allocate buffer
  - Read data to the stream buffer
  - Copy data from stream buffer to destination



Introduction

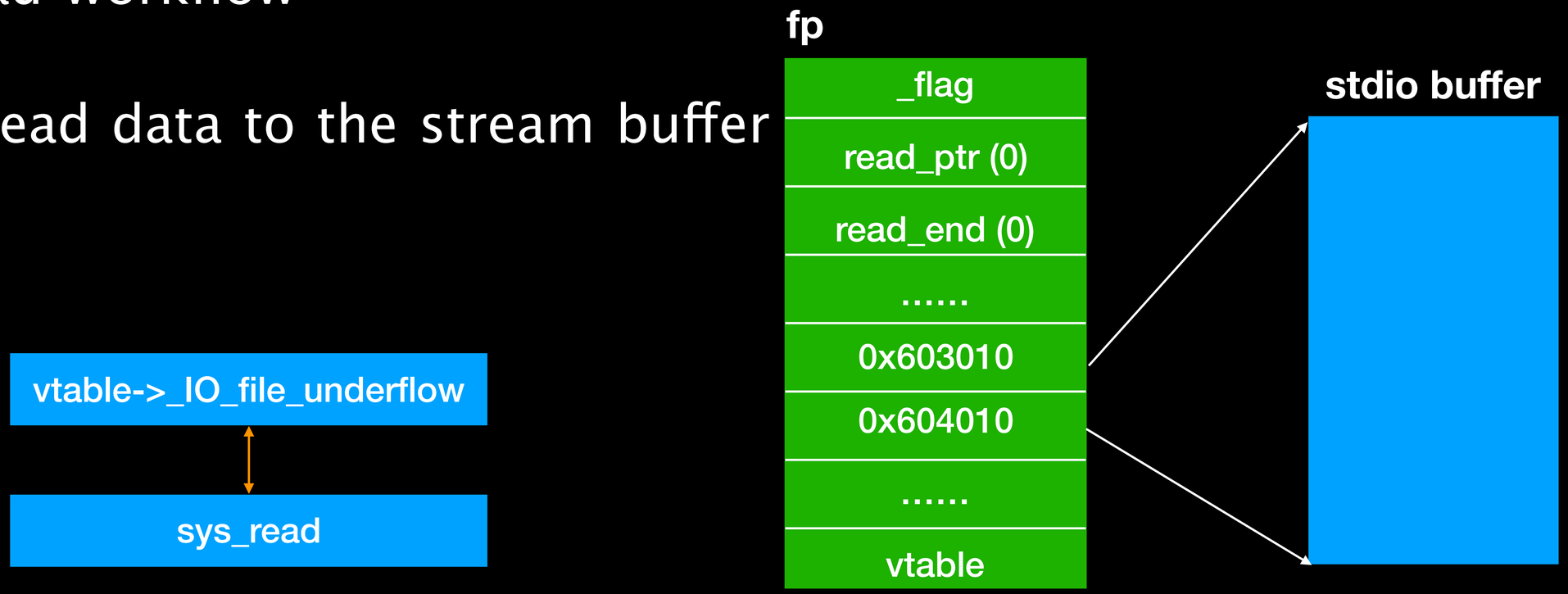
- fread workflow
  - If stream buffer is NULL
    - Allocate buffer





Introduction

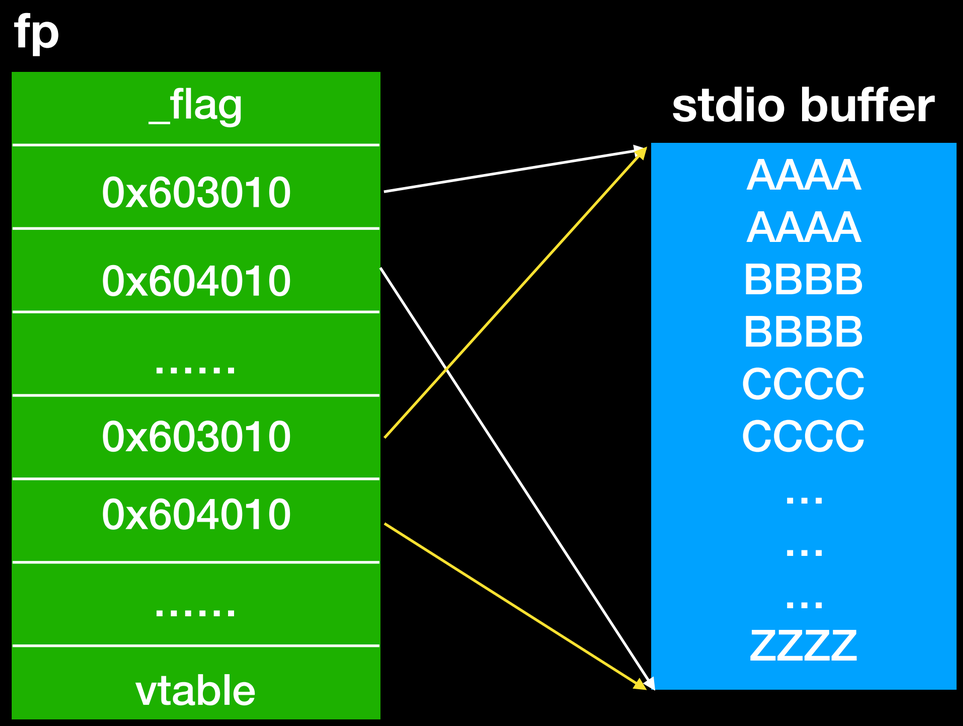
- fread workflow
  - Read data to the stream buffer



Introduction

- fread workflow
  - Copy data from stream buffer to destination

vtable->_IO_file_xsgetn

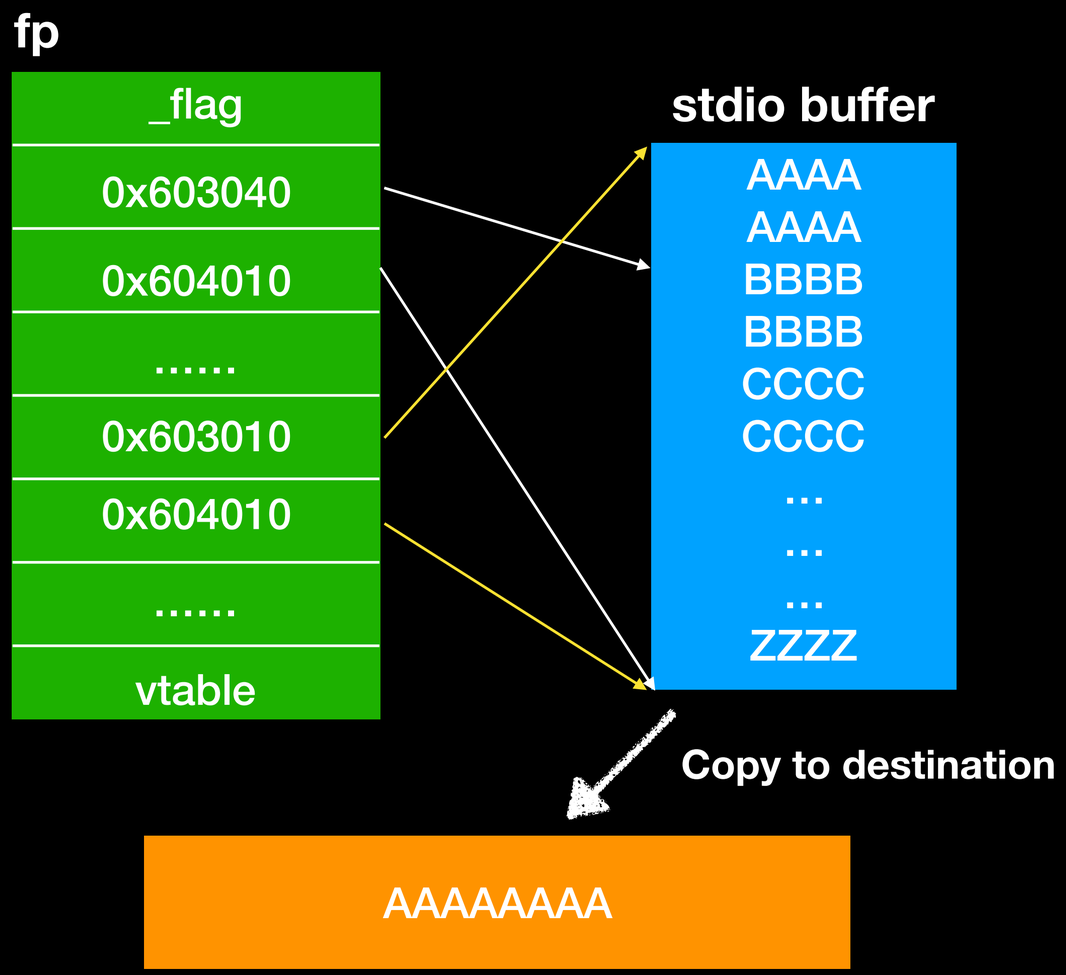


Destination

Introduction

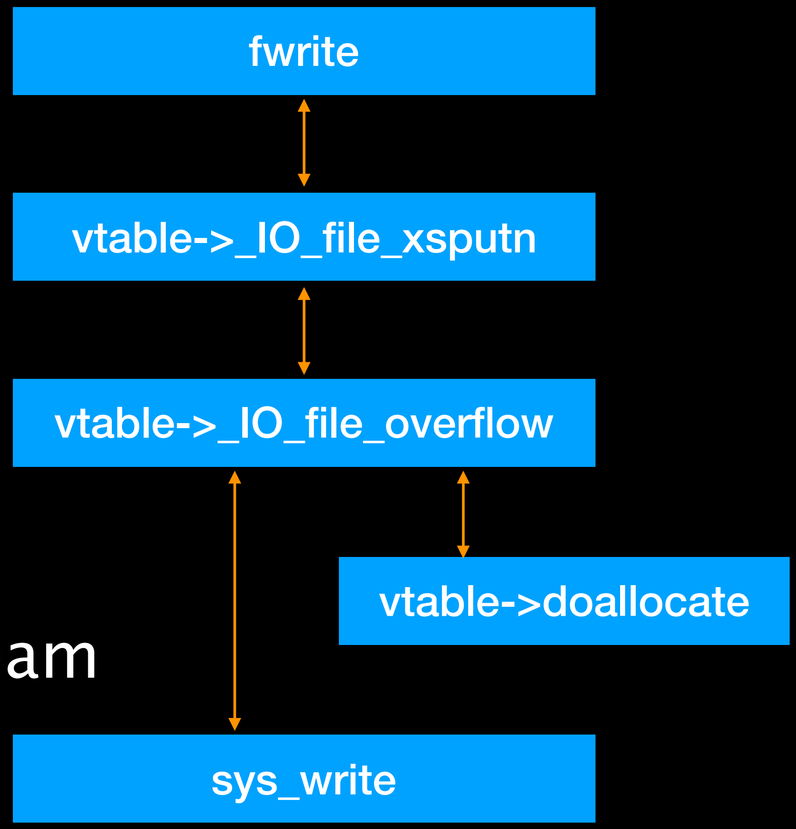
- fread workflow
  - Copy data from stream buffer to destination

vtable->_IO_file_xsgetn



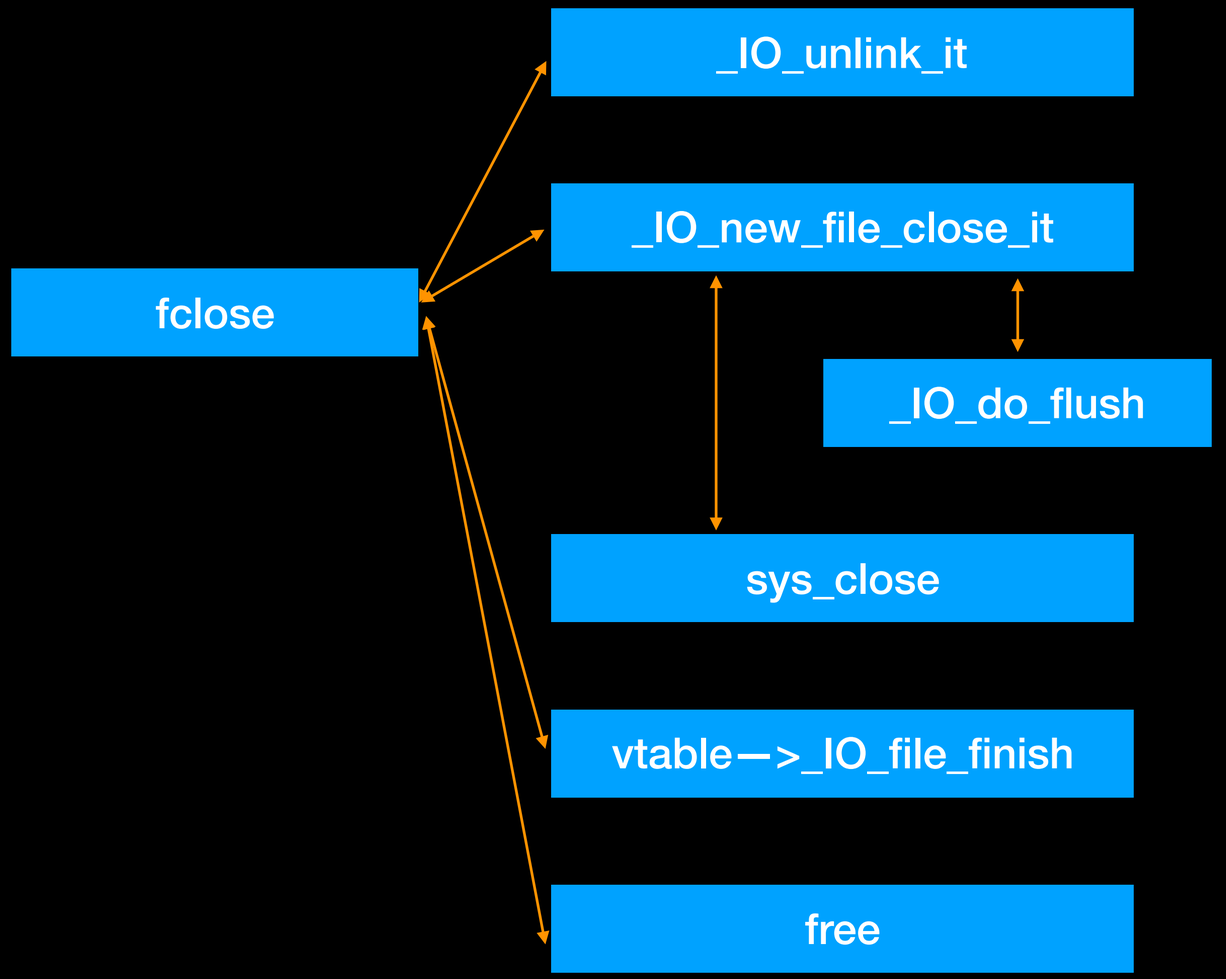
Introduction

- fwrite workflow
  - If stream buffer is NULL
    - Allocate buffer
  - Copy user data to the stream buffer
  - If the stream buffer is filled or flush the stream
    - write data from stream buffer to the file



Introduction

- fclose workflow
  - Unlink the FILE structure
  - Flush & Release the stream buffer
  - Close the file
  - Release the FILE structure



Agenda

- Introduction
  - File stream
  - Overview the FILE structure
- Exploitation of FILE structure
  - FSOP
  - Vtable verification in FILE structure
  - Make FILE structure great again
- Conclusion

Exploitation of FILE

- There are many good targets in FILE structure
  - Virtual Function Table

```
struct _IO_FILE_plus
{
  _IO_FILE file;
  const struct _IO_jump_t *vtable;
};
```

Exploitation of FILE

- Let's overwrite with buffer address

```
char buf[0x100] = {0}; //variable buf at 0x6009a0
FILE *fp ;
int main(){
    fp = fopen("key.txt","rw");
    gets(buf);
    fclose(fp);
}
```

Sample code

Buffer overflow

Buffer address

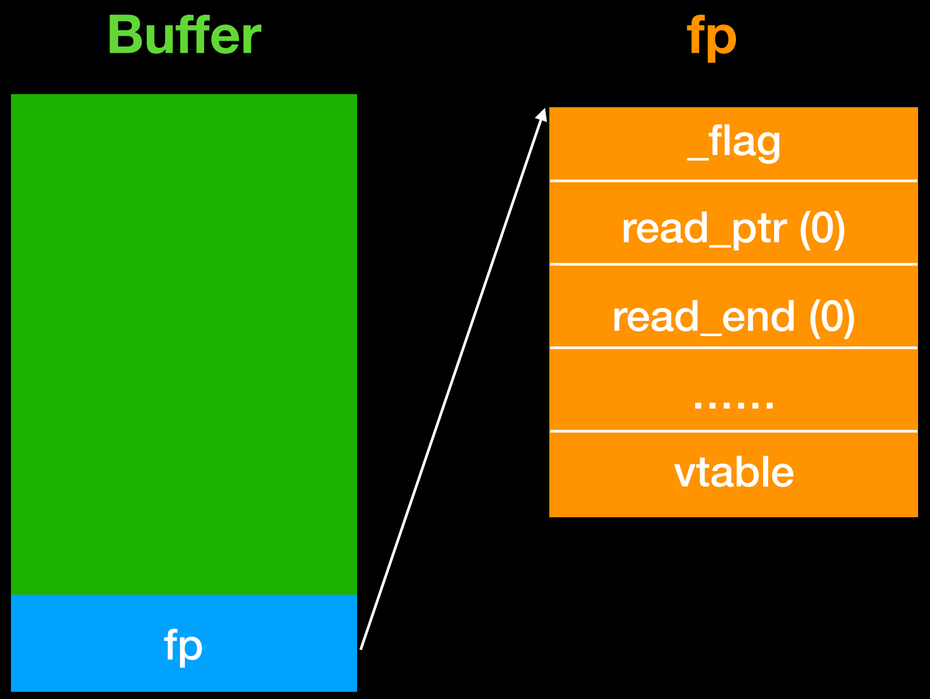
```
payload = "A"*0x100 + p64(0x6009a0)
```

payload

Exploitation of FILE

- Let's overwrite with buffer address

```
char buf[0x100] = {0};
FILE *fp ;
int main(){
    fp = fopen("key.txt","rw");
    gets(buf);
    fclose(fp);
}
```

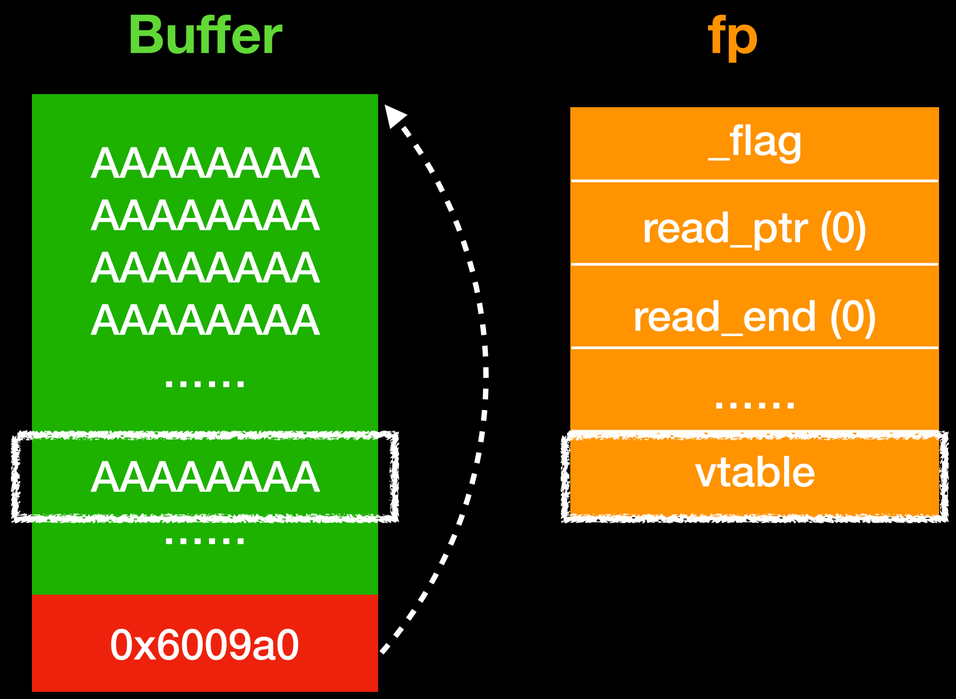


Exploitation of FILE

- Let’s overwrite with buffer address

```
char buf[0x100] = {0};
FILE *fp ;
int main(){
    fp = fopen("key.txt","rw");
    gets(buf);
    fclose(fp);
}
```

Buffer overflow



Exploitation of FILE

- Not call vtable directly…
  - RDX is our input
    but not call instruction

```
RDX: 0x4141414141414141 ('AAAAAAAA')
RSI: 0x601010 ('A' <repeats 200 times>...)
RDI: 0x601010 ('A' <repeats 200 times>...)
RBP: 0x7fffffffe500 --> 0x400600 (<__libc_csu_init>:    push   r15)
RSP: 0x7fffffffe4d0 --> 0x0
RIP: 0x7ffff7a7a38c (<_IO_new_fclose+300>:      cmp    r8,QWORD PTR [rdx
R8 : 0x7ffff7fdd700 (0x00007ffff7fdd700)
R9 : 0x0
R10: 0x477
R11: 0x7ffff7a7a260 (<_IO_new_fclose>:  push   r12)
R12: 0x4004c0 (<_start>:        xor    ebp,ebp)
R13: 0x7fffffffe5e0 --> 0x1
R14: 0x0
R15: 0x0
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction
------------------------------------------------------ Code ------------
   0x7ffff7a7a37a <_IO_new_fclose+282>: jne    0x7ffff7a7a3d6 <_IO_new_f
   0x7ffff7a7a37c <_IO_new_fclose+284>: mov    rdx,QWORD PTR [rbx+0x88]
   0x7ffff7a7a383 <_IO_new_fclose+291>: mov    r8,QWORD PTR fs:0x10
=> 0x7ffff7a7a38c <_IO_new_fclose+300>: cmp    r8,QWORD PTR [rdx+0x8]
   0x7ffff7a7a390 <_IO_new_fclose+304>: je     0x7ffff7a7a3d2 <_IO_new_f
```

Exploitation of FILE

- Let’s see what happened in fclose
  - We can get information of segfault in gdb and located it in source code

```
37 int
38 _IO_new_fclose (_IO_FILE *fp)
39 {
40   int status;
41   ...
42   _IO_acquire_lock (fp);
43   if (fp->_IO_file_flags & _IO_IS_FILEBUF)
44     status = _IO_file_close_it (fp);
45   ...
46 }
```

Exploitation of FILE

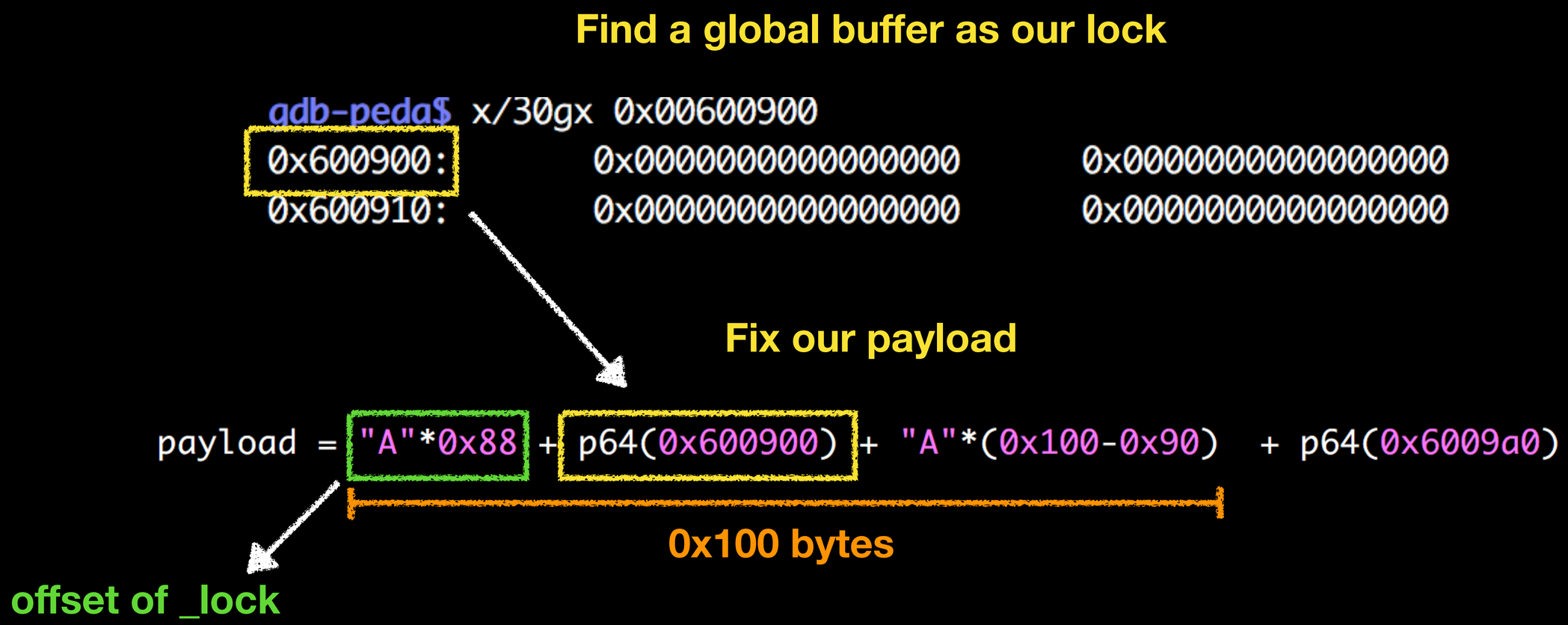
- FILE structure
  - _lock
  - Prevent race condition in multithread
  - Very common in stdio related function
  - Usually need to construct it for Exploitation

```
typedef struct { int lock; int cnt; void *owner; } _IO_lock_t;
```

```
struct _IO_FILE {
  int _flags;   /* High-order
  ...
  char* _IO_read_ptr; /* Curr
  ...
  char _shortbuf[1];
  ...

  _IO_lock_t *_lock;
#ifdef _IO_USE_OLD_IO_FILE
};
```

Exploitation of FILE

- Let's fix the lock



Exploitation of FILE

- We control PC !

```
RAX: 0x4141414141414141 ('AAAAAAAA')
RBX: 0x6009a0 ('A' <repeats 136 times>)
RCX: 0x7f55b6de28e0 --> 0xfbad2088
RDX: 0x600900 --> 0x0
RSI: 0x0
RDI: 0x6009a0 ('A' <repeats 136 times>)
RBP: 0x0
RSP: 0x7ffee6b936c0 --> 0x0
RIP: 0x7f55b6a8b29c (<_IO_new_fclose+60>:        call   QWORD PTR [rax+
R8 : 0x7f55b6ff2700 (0x00007f55b6ff2700)
R9 : 0x4141414141414141 ('AAAAAAAA')
R10: 0x477
R11: 0x7f55b6a8b260 (<_IO_new_fclose>:  push   r12)
R12: 0x400470 (<_start>:        xor    ebp,ebp)
R13: 0x7ffee6b937c0 --> 0x1
R14: 0x0
R15: 0x0
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT directic
-------------------------------------------------------------------
-------------------------------
   0x7f55b6a8b290 <_IO_new_fclose+48>:  mov    rax,QWORD PTR [rbx+0xd8
   0x7f55b6a8b297 <_IO_new_fclose+55>:  xor    esi,esi
   0x7f55b6a8b299 <_IO_new_fclose+57>:  mov    rdi,rbx
=> 0x7f55b6a8b29c <_IO_new_fclose+60>:  call   QWORD PTR [rax+0x10]
```

Exploitation of FILE

- Another interesting
  - stdin/stdout/stderr is also a FILE structure in glibc
  - We can overwrite the global variable in glibc to control the flow

```
00000000003c48e0 g    DO .data  00000000000000e0  GLIBC_2.2.5 _IO_2_1_stdin_
00000000003c5710 g    DO .data  0000000000000008  GLIBC_2.2.5 stdin
00000000003c5620 g    DO .data  00000000000000e0  GLIBC_2.2.5 _IO_2_1_stdout_
00000000003c5708 g    DO .data  0000000000000008  GLIBC_2.2.5 stdout
00000000003c5700 g    DO .data  0000000000000008  GLIBC_2.2.5 stderr
```

GLIBC SYMBOL TABLE

Global offset

Lab 12-1

- Seethefile

Agenda

- Introduction
  - File stream
  - Overview the FILE structure
- Exploitation of FILE structure
  - FSOP
  - Vtable verification in FILE structure
  - Make FILE structure great again
- Conclusion

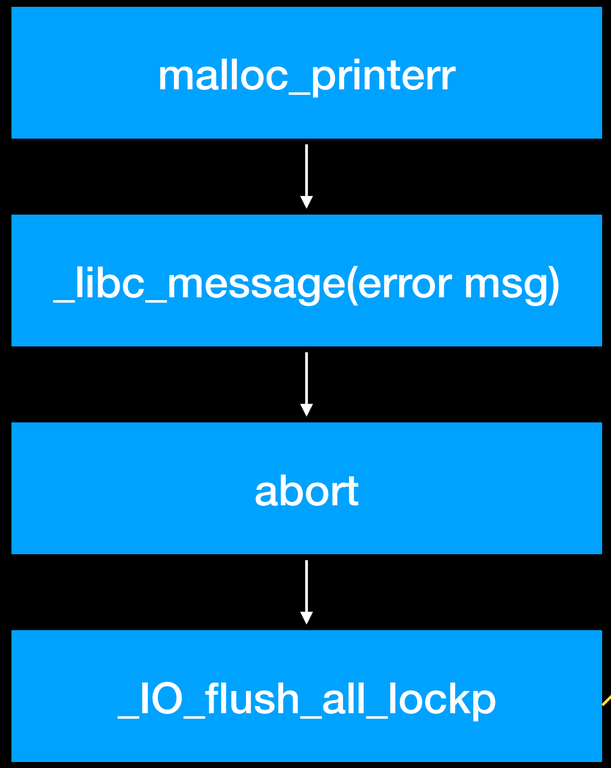
FSOP

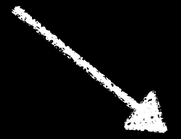
- File-Stream Oriented Programing
  - Control the linked list of File stream
    - _chain
    - _IO_list_all
  - Powerful function
    - **_IO_flush_all_lockp**

FSOP

- _IO_flush_all_lockp
  - fflush all file stream
- When will call it
  - Glib abort routine
  - exit function
  - Main return

Glibc abort routine





If the condition is satisfied

FSOP

- _IO_flush_all_lockp
  - It will process all FILE in FILE linked list
  - We can construct the linked list to do oriented programing

```
_IO_flush_all_lockp (int do_lock)
{
  struct _IO_FILE *fp;
  ...
  fp = (_IO_FILE *) _IO_list_all;
  while (fp != NULL)
    {
      run_fp = fp;
      if (((fp->_mode <= 0 &&
        fp->_IO_write_ptr > fp->_IO_write_base))
      && _IO_OVERFLOW (fp, EOF) == EOF)
      result = EOF;
      run_fp = NULL;
    ...
      fp = fp->_chain;
    }
    ...
  return result;
}
```

fp = _IO_list_all

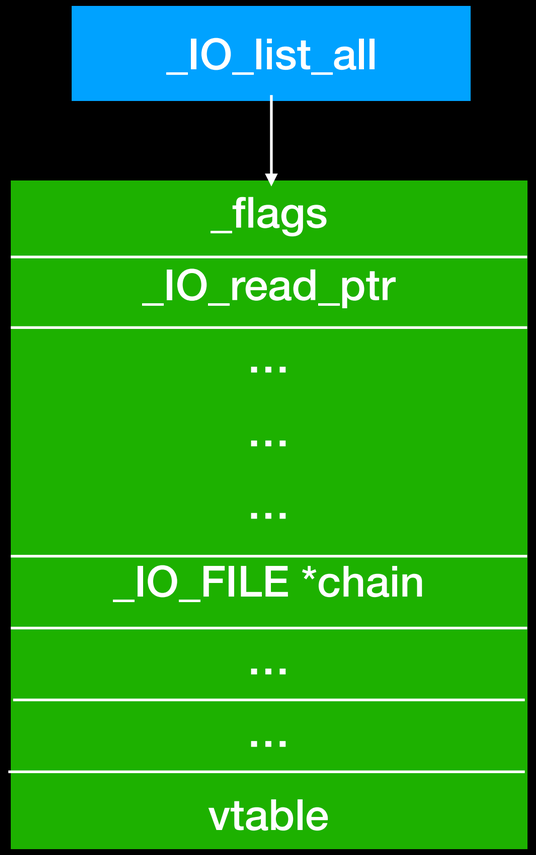
condition

Trigger virtual funcition

Point to next

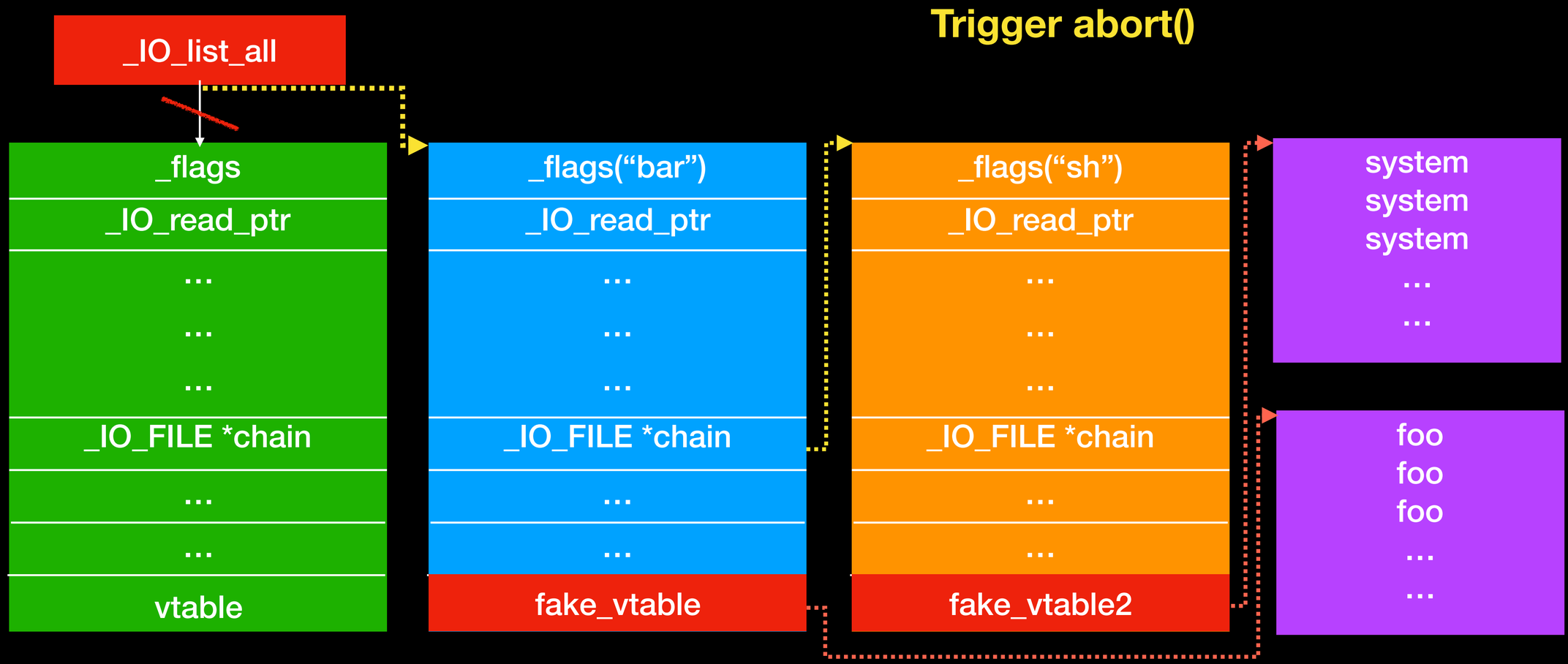
FSOP

- File-Stream Oriented Programing



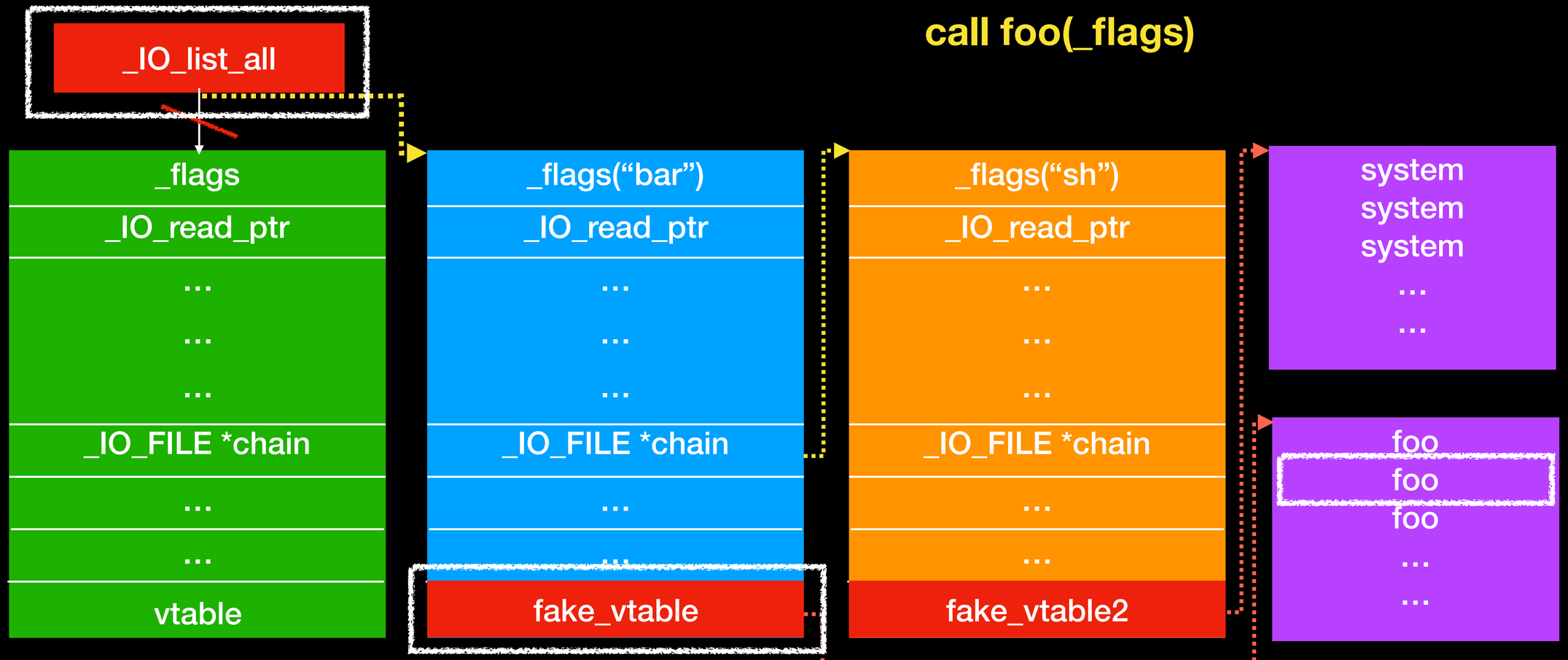
FSOP

- File-Stream Oriented Programing



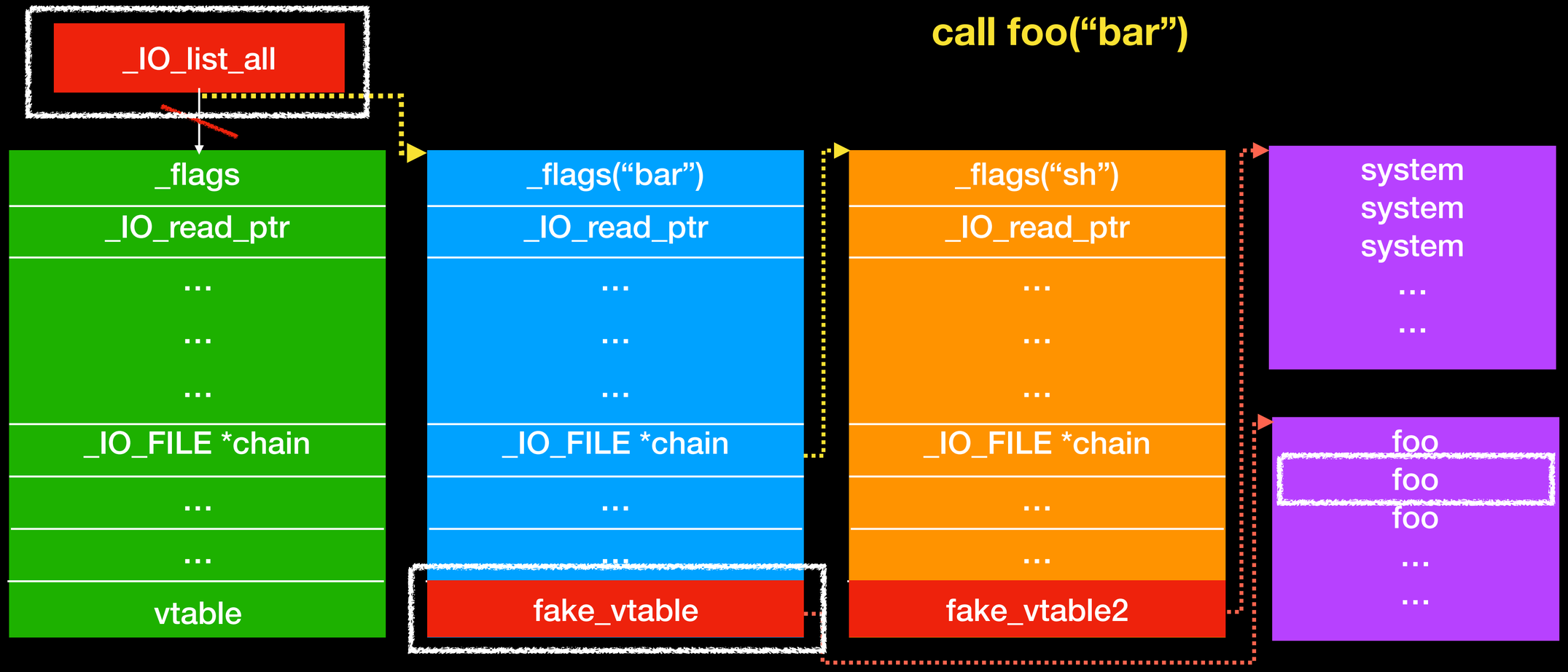
FSOP

- File-Stream Oriented Programing



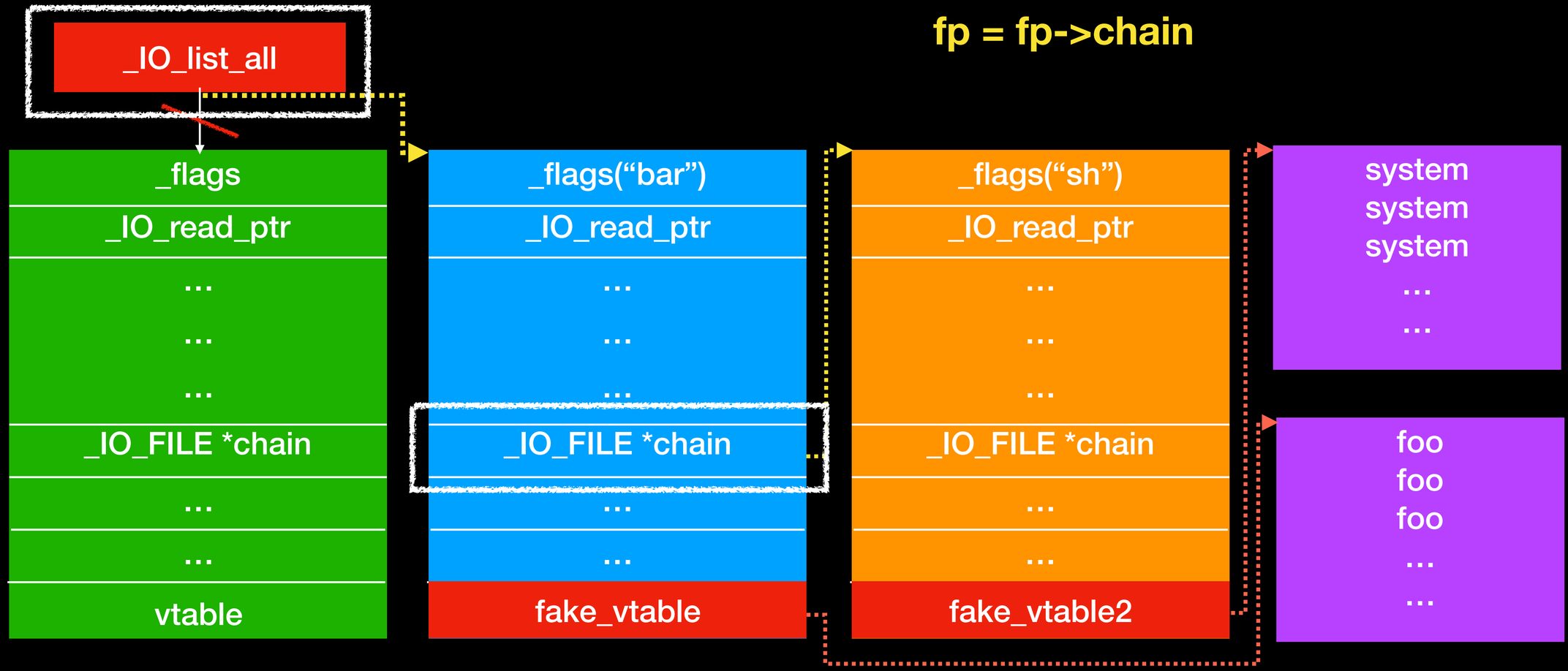
FSOP

- File-Stream Oriented Programing



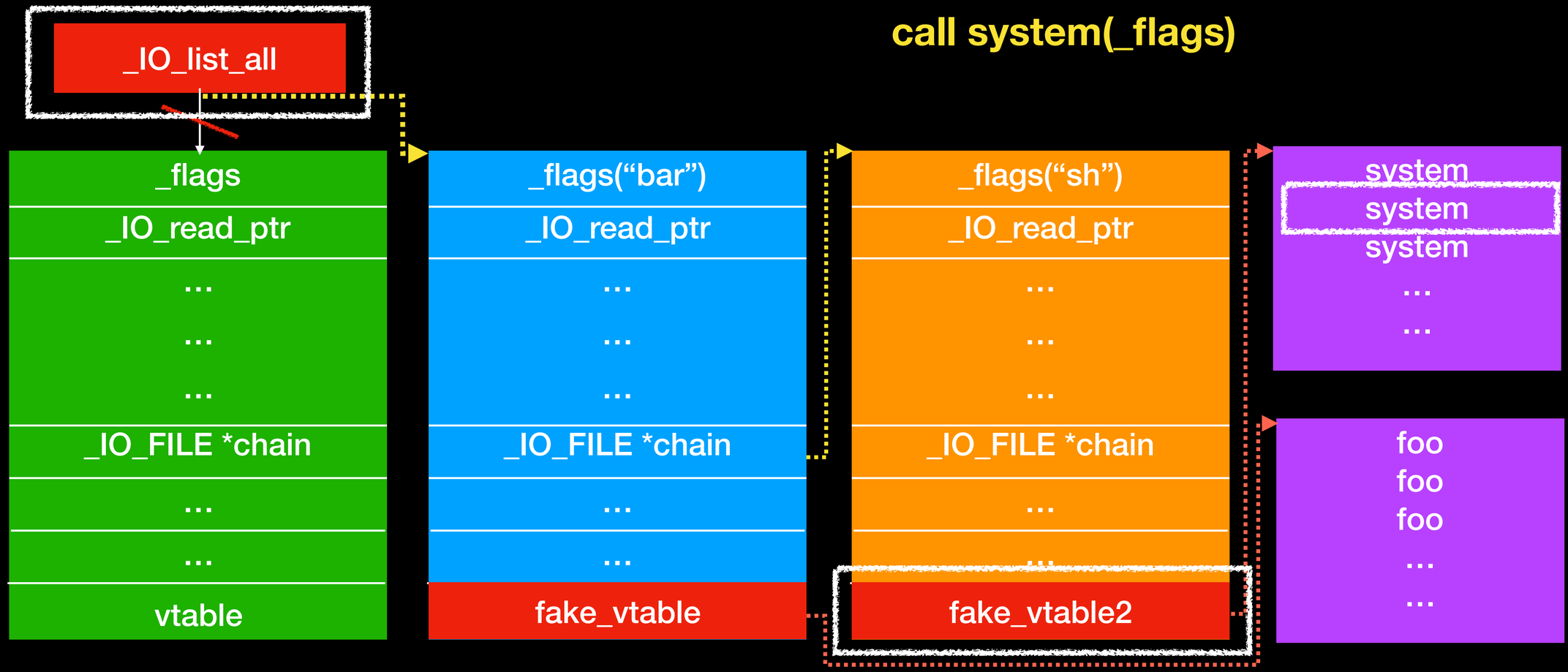
FSOP

- File-Stream Oriented Programing



FSOP

- File-Stream Oriented Programing



FSOP

- File-Stream Oriented Programing

House of Orange

- 利用 Unsorted bin attack 將 unsorted bin 位置寫入 _IO_list_all
  - 同時也構造出 0x60 大小的 chunk 進入 small bin
  - 最後觸發 _IO_flush_all_lockp
    - 會有 1/2 機率將會把 0x60 大小的 chunk 當作 FILE Structure 進而達成 FSOP

House of Orange

- Unsorted bin attack
  - 在 malloc 時，不論 unsorted bin 是否有剛好大小的 chunk ，都會對 unsorted bin 的 chunk 做 unlink
    - 有剛好大小，從 unsorted bin 移除給使用者
    - 不是剛好大小，從 unsorted bin 移除，放到相對應的 bin 中

Unsorted bin attack

- 但這個 unlink 跟平常的 unlink 方式有點不同，並沒有針對 double linked list 做檢查

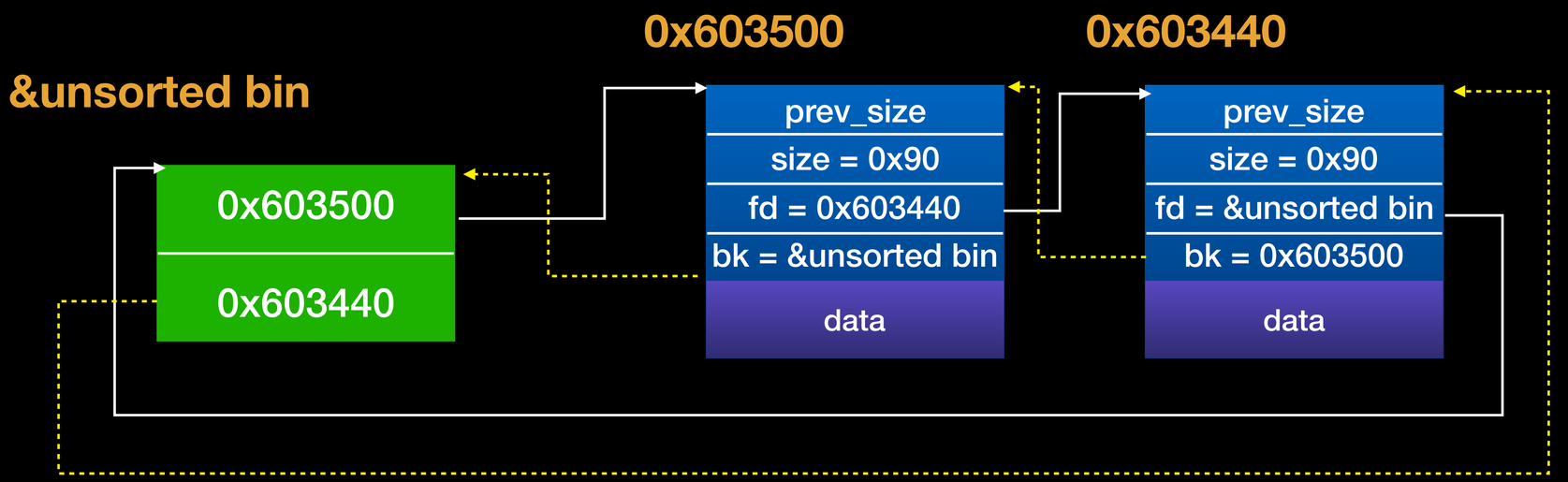
- 移除時會先取出 unsorted bin 最後一塊 chunk 做為 victim，然後將這一塊的 bk 指向的 chunk 的 fd 改成 unsorted bin 位置

```
int iters = 0;
while ((victim = unsorted_chunks (av)->bk) != unsorted_chunks (av))
  {
    bck = victim->bk;

    /* remove from unsorted list */
    unsorted_chunks (av)->bk = bck;
    bck->fd = unsorted_chunks (av);
```

Unsorted bin attack

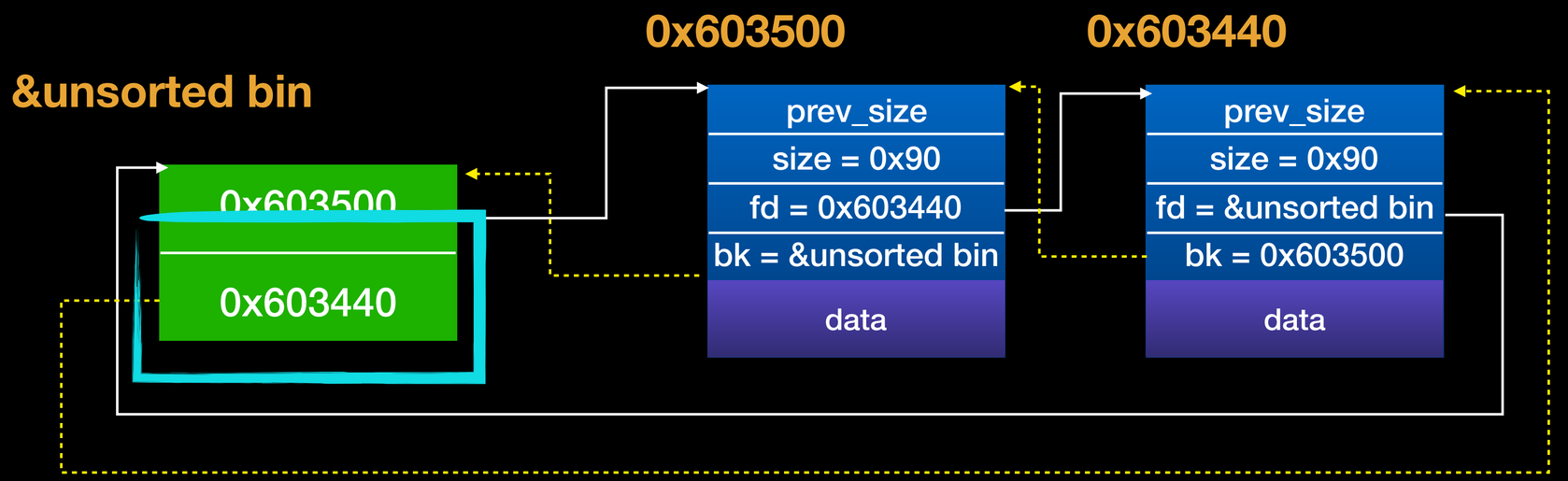
- 所以只要將最後一塊的 bk 改寫成任意位置，就可以在任意位置上寫上 unsorted bin 的位置
  - 理論上會是一個很大的數字
  - 通常會寫道 glibc 中 global_max_fast 這個變數，該變數主要用來判斷是否為 fastbin 的 chunk ，如果 chunk size 小於這變數就會認為是 fastbin
  - 可以配合 fastbin corruption attack

Process unsorted chunks



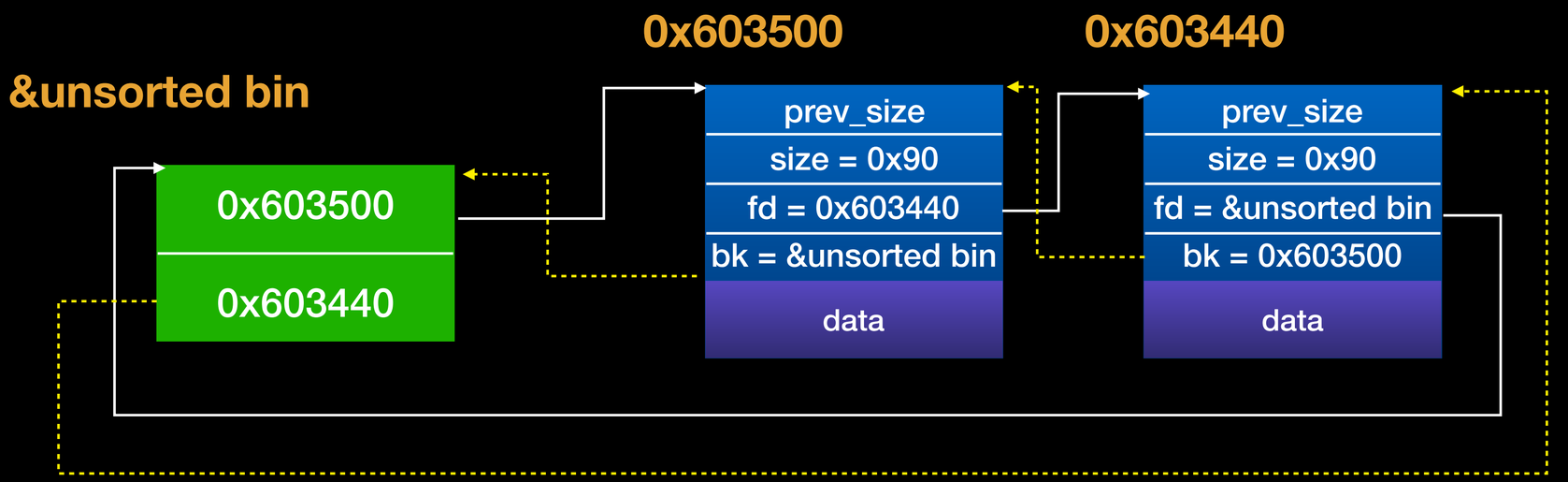
- call malloc(0x80)
  - remove the 0x603440 from unsorted bin
  - return 0x603450 to user

Process unsorted chunks



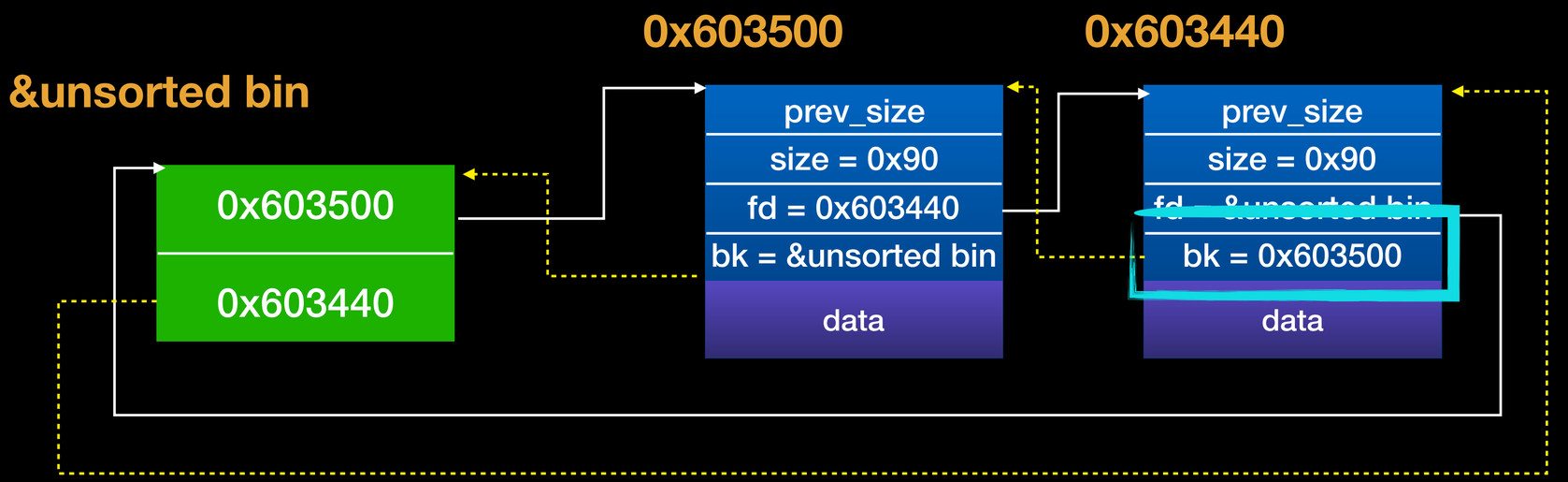
- victim = unsorted_chunks(av)->bk

Process unsorted chunks



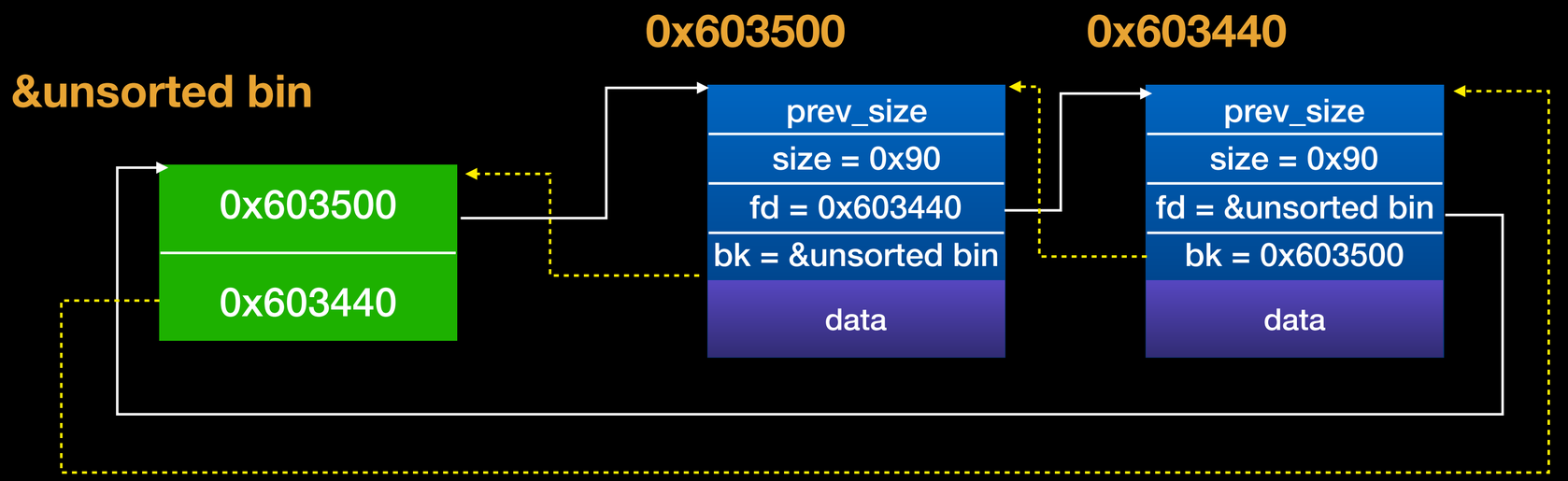
- victim = unsorted_chunks(av)->bk
- victim = 0x603440

Process unsorted chunks



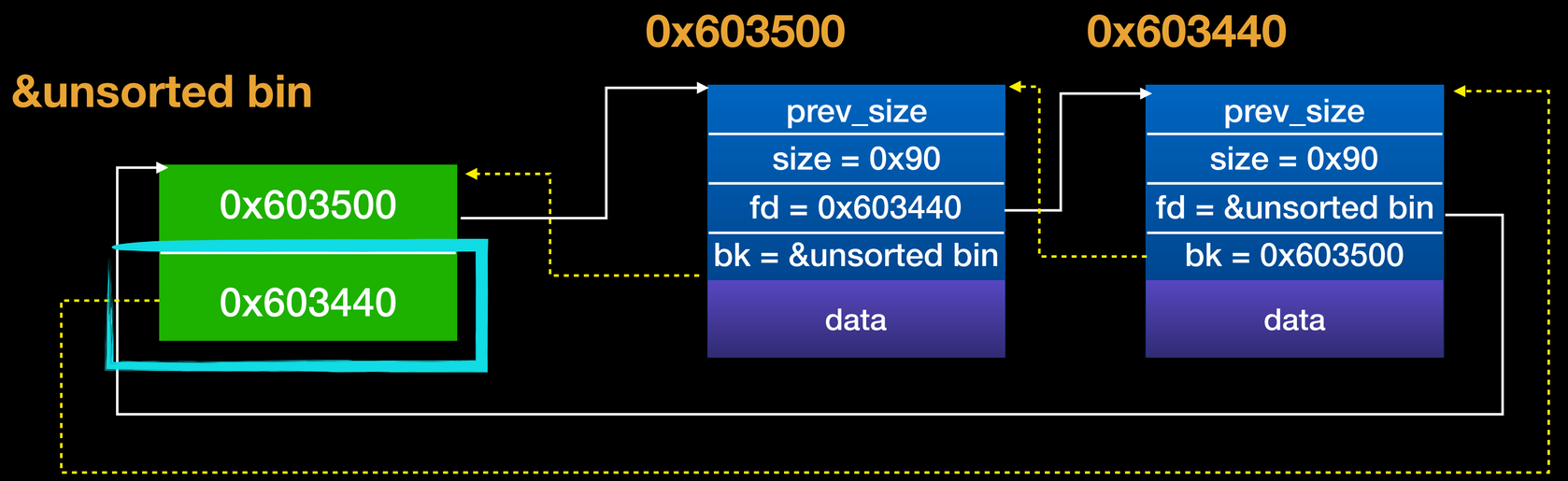
- victim = 0x603440
- bck = victim->bk

Process unsorted chunks



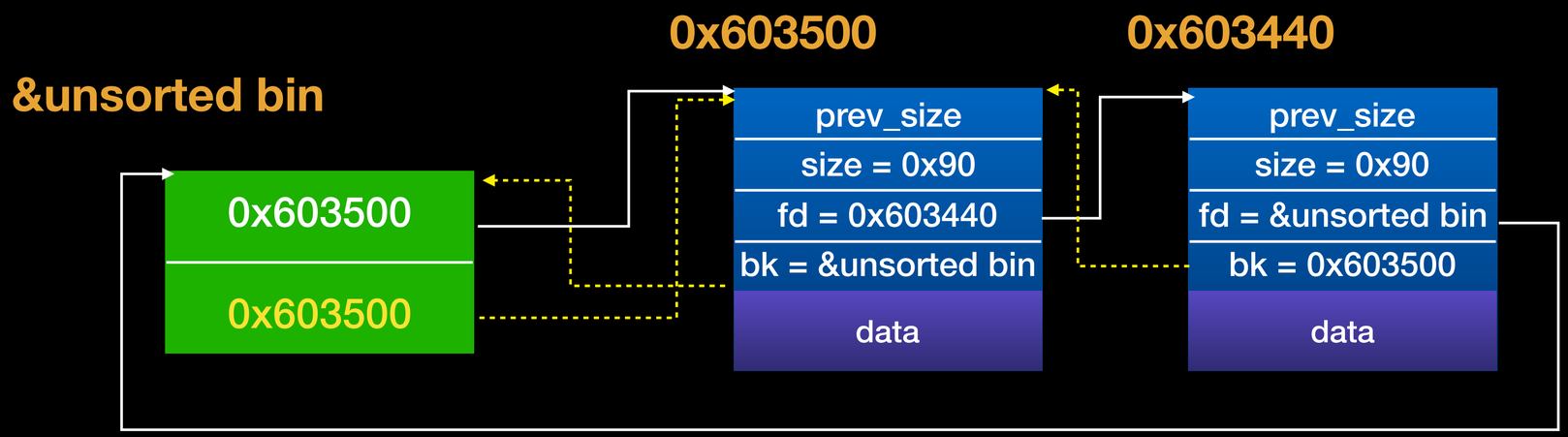
- victim = 0x603440
- bck = 0x603500

Process unsorted chunks



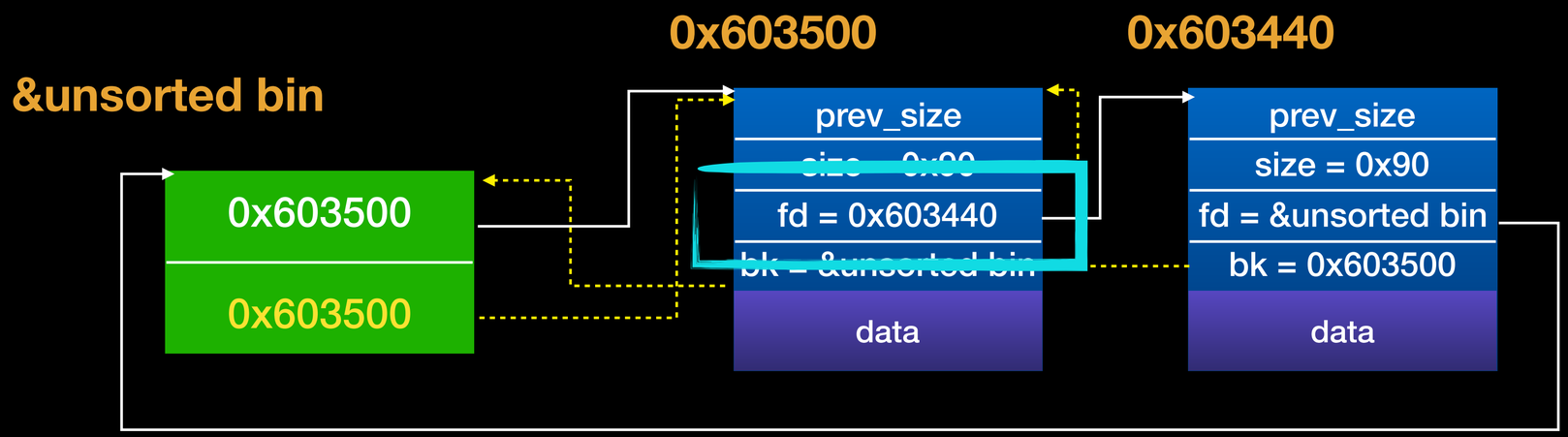
- bck = 0x603500
- unsorted_chunks(av)->bk = bck

Process unsorted chunks



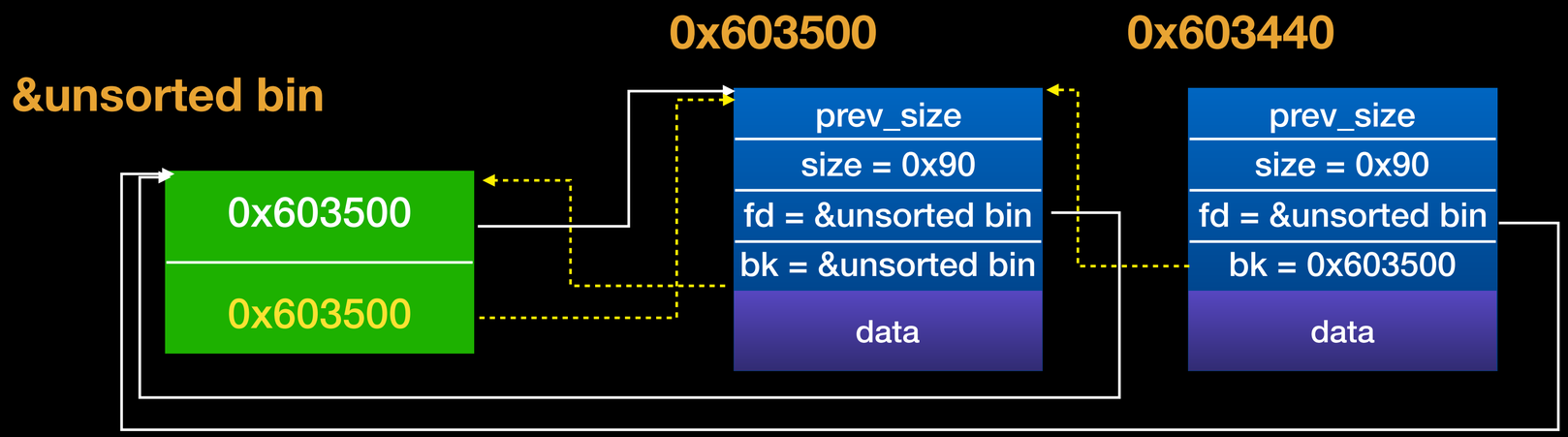
- bck = 0x603500
- unsorted_chunks(av)->bk = bck

Process unsorted chunks



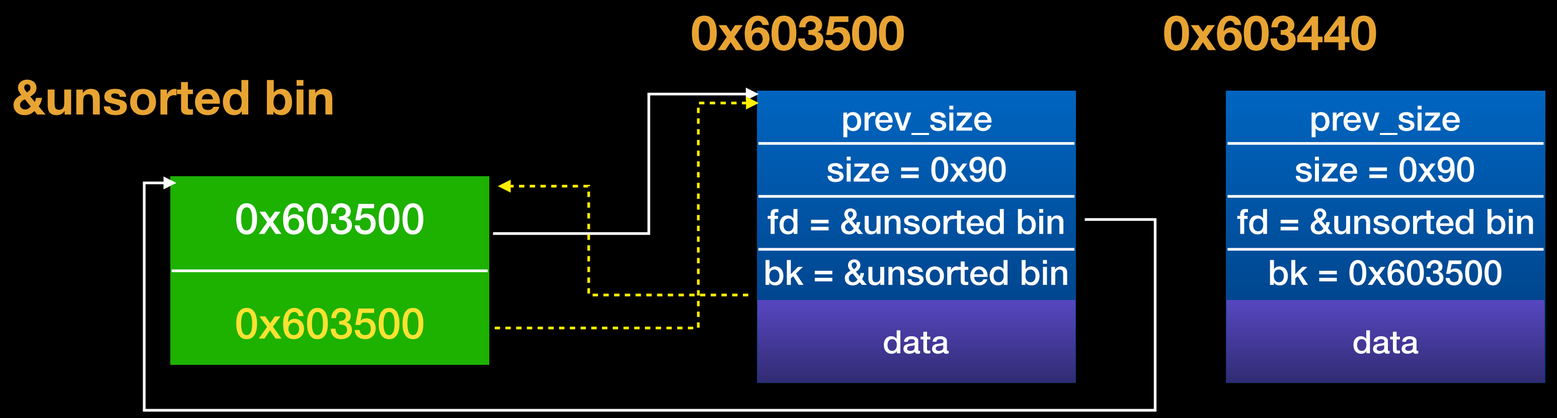
- bck = 0x603500
- unsorted_chunks(av)->bk = bck
- bck->fd = unsorted_chunks(av)

Process unsorted chunks



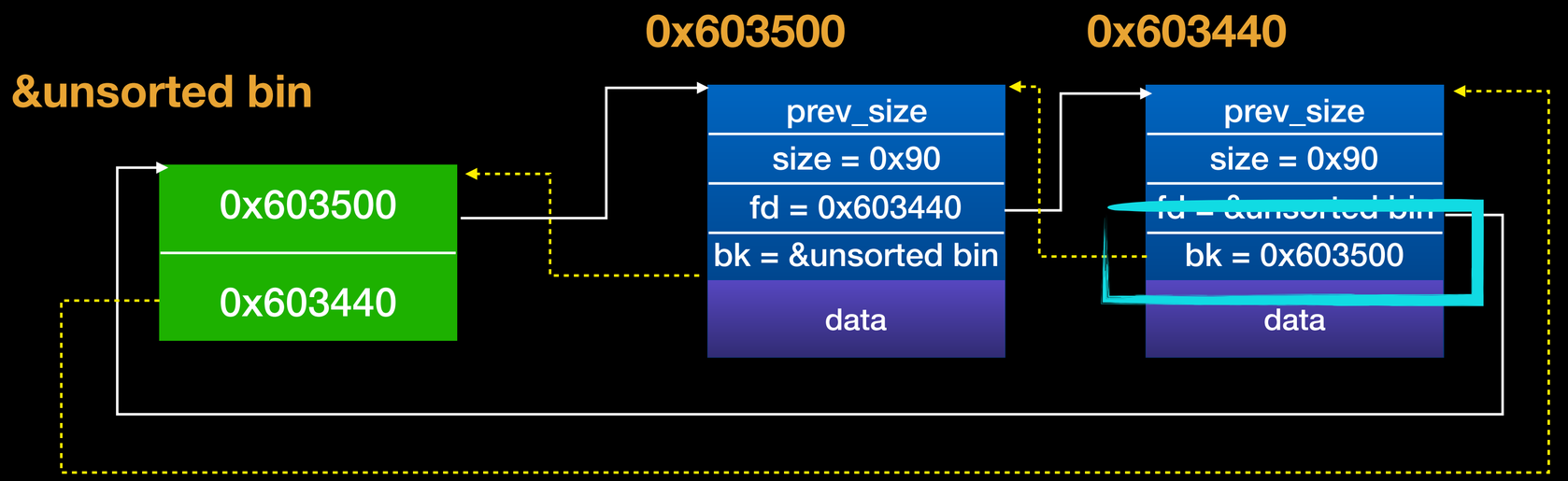
- bck = 0x603500
- unsorted_chunks(av)->bk = bck
- bck->fd = unsorted_chunks(av)

Process unsorted chunks



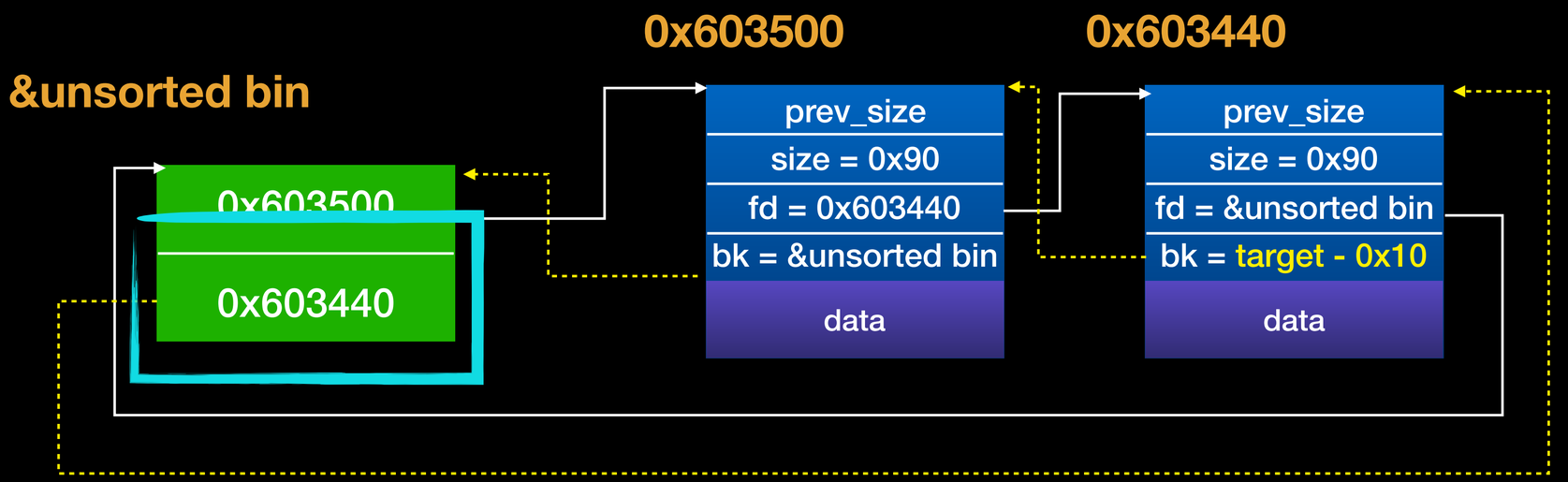
- Return 0x603450 to user
- If (nb != victim->size)
  - put 0x603440 to smallbin

Unsorted bin attack



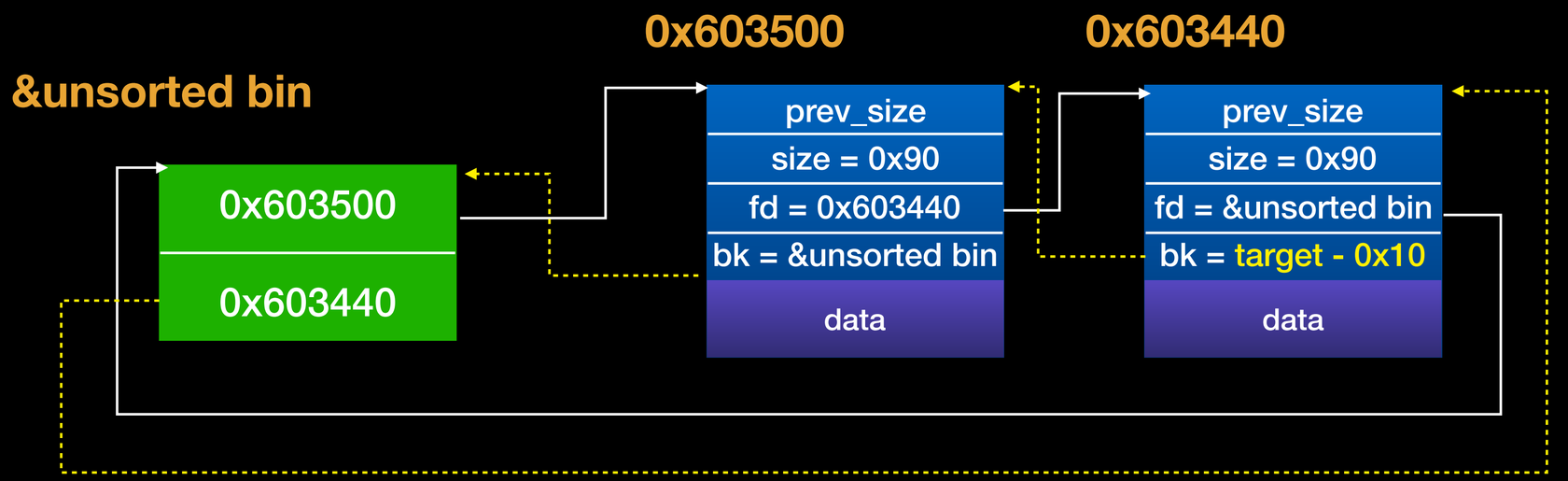
- Corruption in 0x603440

Unsorted bin attack



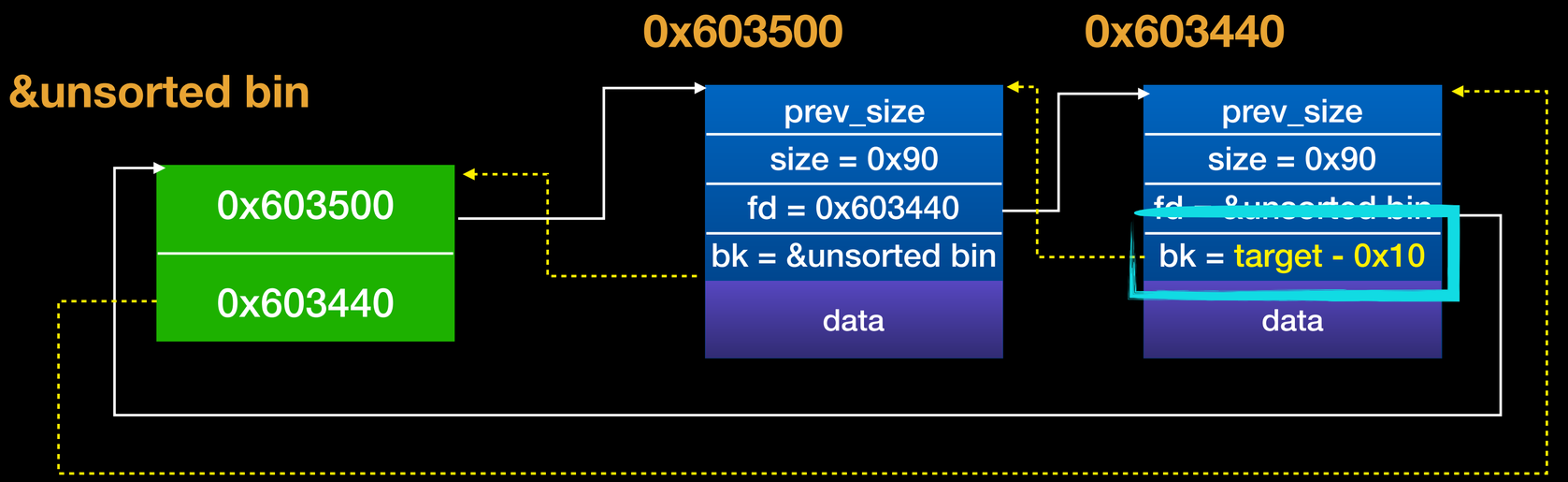
- victim = unsorted_chunks(av)->bk

Unsorted bin attack



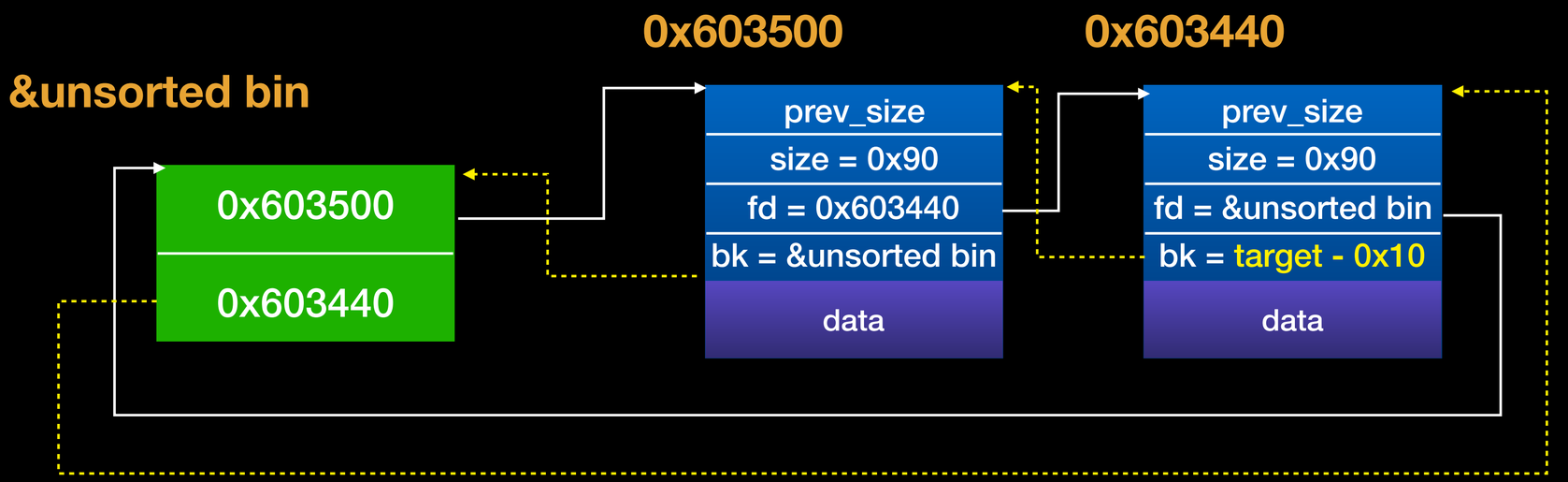
- victim = unsorted_chunks(av)->bk
- victim = 0x603440

Unsorted bin attack



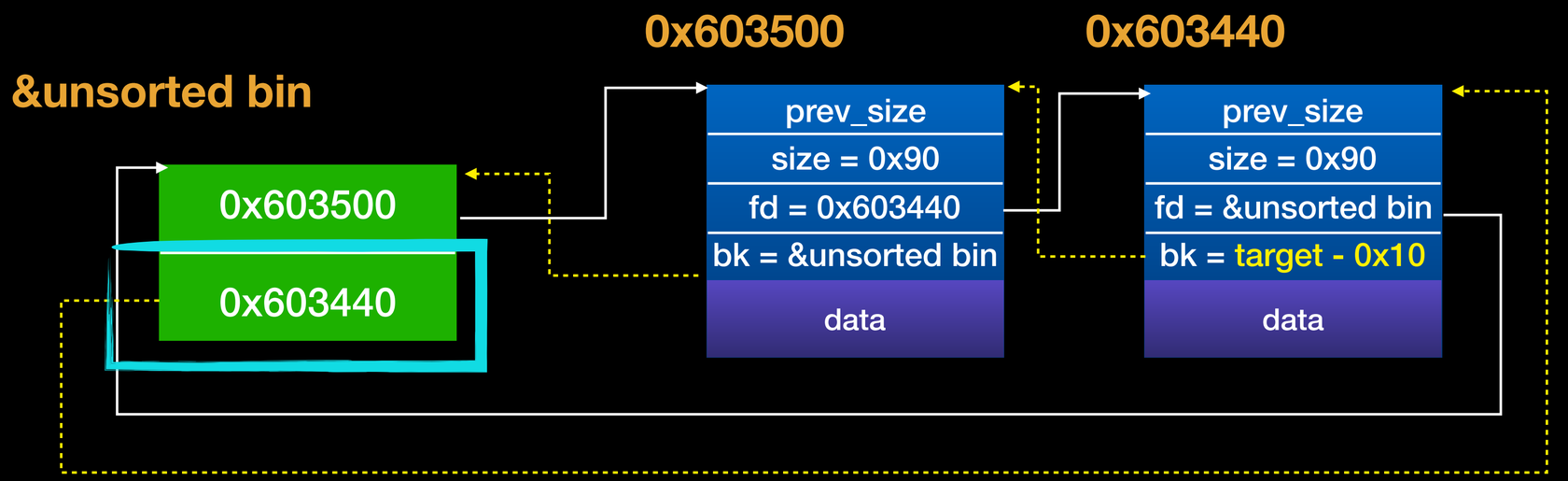
- victim = 0x603440
- bck = victim->bk

Unsorted bin attack



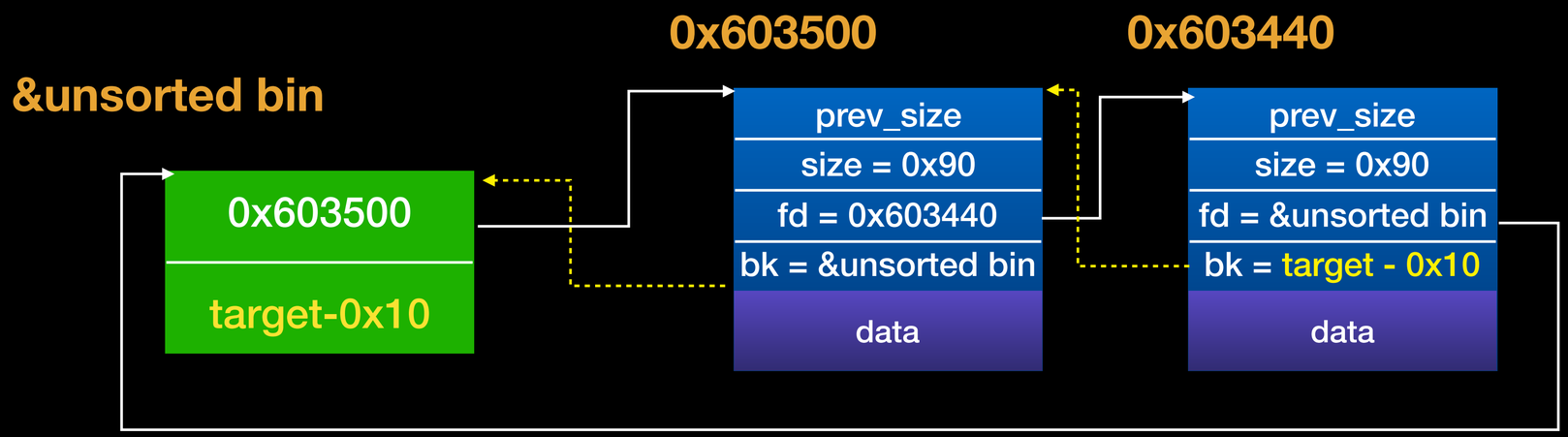
- victim = 0x603440
- bck = target - 0x10

Unsorted bin attack



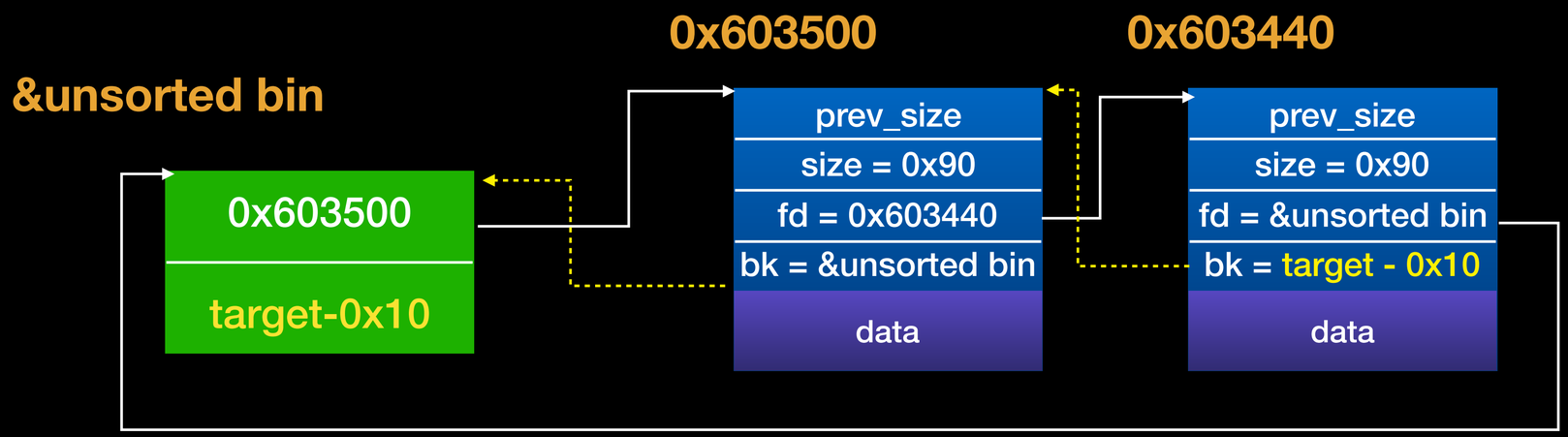
- bck = target - 0x10
- unsorted_chunks(av)->bk = bck

Unsorted bin attack



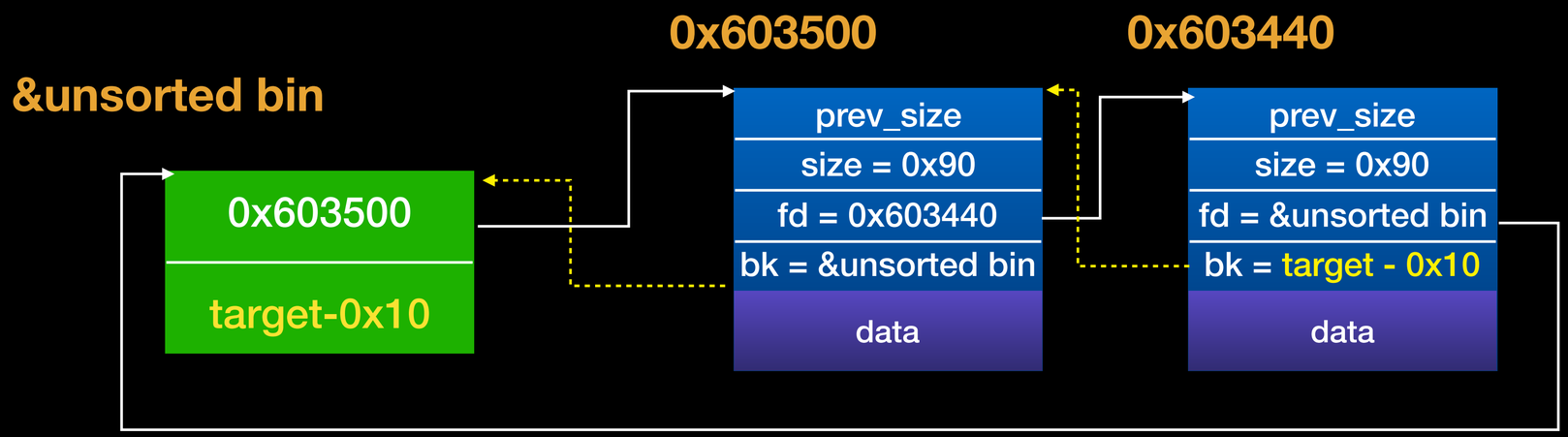
- bck = target - 0x10
- unsorted_chunks(av)->bk = bck

Unsorted bin attack



- bck = target - 0x10
- unsorted_chunks(av)->bk = bck
- bck->fd = unsored_chunks(av)

Unsorted bin attack



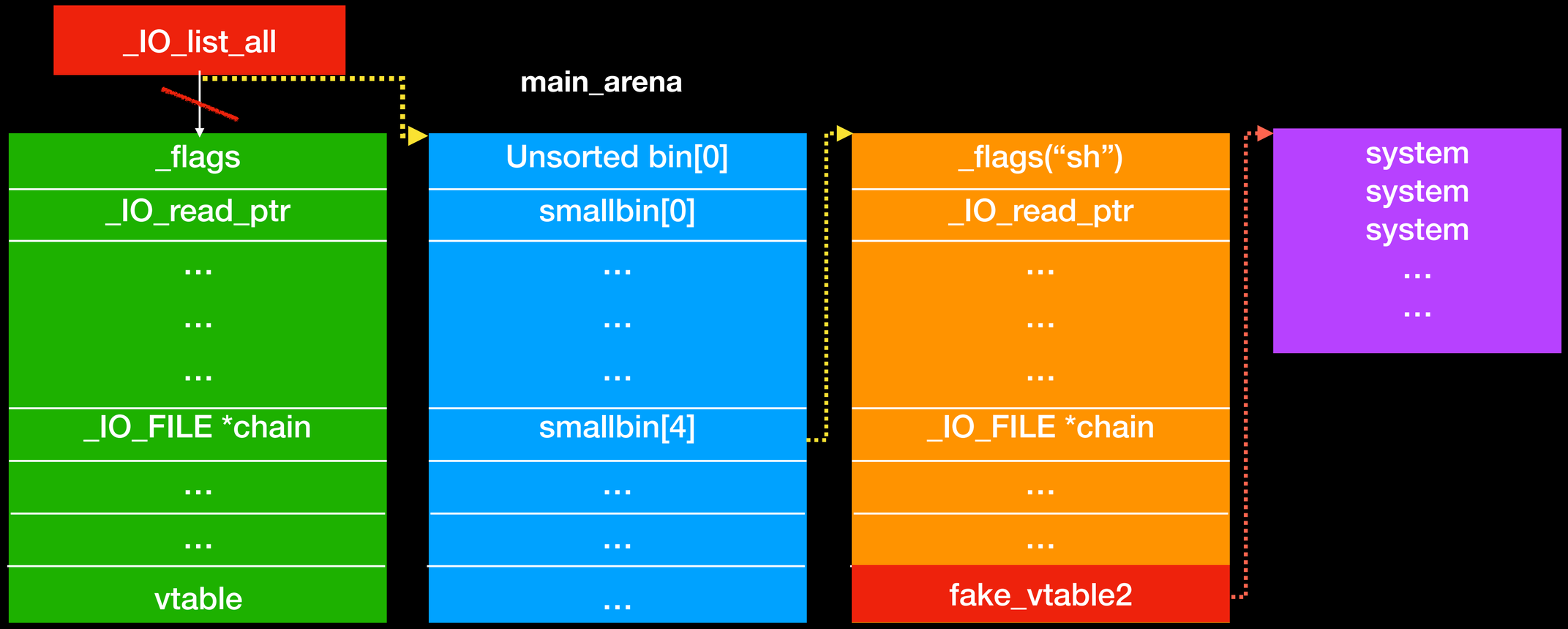
- target = unsorted_chunks(av)
- if target == global_fast_max
  - global_fast_max = unsorted_chunks(av)

Lab 12-2

- magicheap

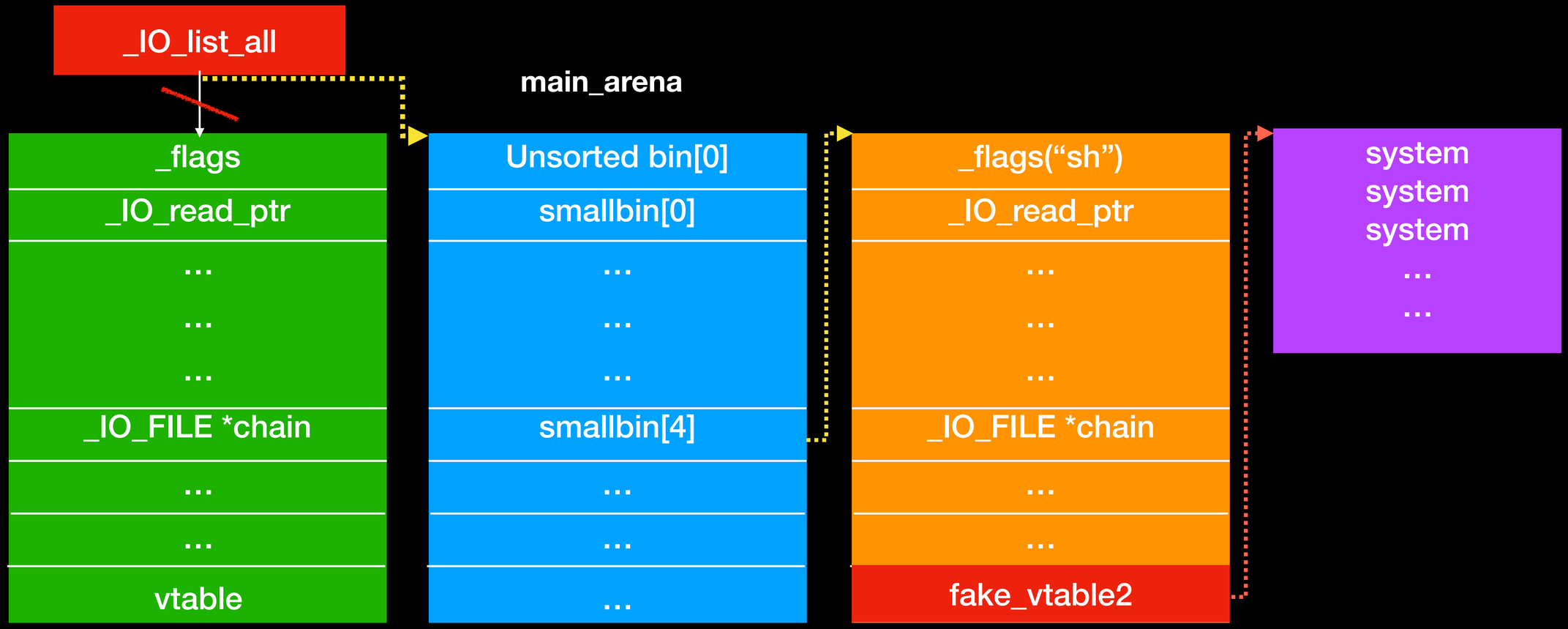
House of Orange

- 利用 Unsorted bin attack 將 unsorted bin 位置寫入 _IO_list_all



House of Orange

- 只要 unsorted bin address (_flags) < 0 就可以讓 _IO_flush_all_lockp 呼叫到我們偽造的 virtual function



Lab 12-3

- Magic Allocator

Agenda

- Introduction
  - File stream
  - Overview the FILE structure
- Exploitation of FILE structure
  - FSOP
  - Vtable verification in FILE structure
  - Make FILE structure great again
- Conclusion

Vtable verification

- Unfortunately, there is a protection added to virtual function table in latest libc
  - Check the address of vtable before all virtual function call
  - If vtable is invalid, it would abort

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Fatal error: glibc detected an invalid stdio handle
Aborted (core dumped)
```

Vtable verification

- Vtable verification in File
  - The vtable must be in libc _IO_vtable section
  - If it's not in _IO_vtable section, it will check if the vtable permits virtual function call

```
static inline const struct _IO_jump_t *
IO_validate_vtable (const struct _IO_jump_t *vtable)
{

  uintptr_t section_length = __stop___libc_IO_vtables - __start___libc_IO_vtables;
  const char *ptr = (const char *) vtable;
  uintptr_t offset = ptr - __start___libc_IO_vtables;
  if (__glibc_unlikely (offset >= section_length))
    _IO_vtable_check ();
  return vtable;
}
```

Vtable verification

- _IO_vtable_check
  - Check the foreign vtables

```
void attribute_hidden
_IO_vtable_check (void)
{
  void (*flag) (void) = atomic_load_relaxed (&IO_accept_foreign_vtables);
  PTR_DEMANGLE (flag);
  if (flag == &_IO_vtable_check)
    return;
  ...
    Dl_info di;
    struct link_map *l;
    if (_dl_open_hook != NULL
        || (_dl_addr (_IO_vtable_check, &di, &l, NULL) != 0
            && l->l_ns != LM_ID_BASE))
      return;
  ...
  __libc_fatal ("Fatal error: glibc detected an invalid stdio handle\n");
}
```

For compatibility

For shared library

Vtable verification

- Bypass ?
  - Overwrite IO_accept_foreign_vtables ?

```
void (*flag) (void) = atomic_load_relaxed (&IO_accept_foreign_vtables);
PTR_DEMANGLE (flag);
if (flag == &_IO_vtable_check)
  return;
```

Vtable verification

- Bypass ?
  - Overwrite IO_accept_foreign_vtables ?
    - It’s very difficult because of the pointer guard

```
void (*flag) (void) = atomic_load_relaxed (&IO_accept_foreign_vtables);
PTR_DEMANGLE (flag);
if (flag == &_IO_vtable_check)
  return;
```

Demangle with pointer guard

Vtable verification

- Bypass ?
  - Overwrite _dl_open_hook ?

```
if (_dl_open_hook != NULL
    || (_dl_addr (_IO_vtable_check, &di, &l, NULL) != 0
        && l->l_ns != LM_ID_BASE))
  return;
```

Vtable verification

- Bypass ?
  - Overwrite _dl_open_hook ?
    - Sounds good, but if you can control the value, you can also control other good target

```
if (_dl_open_hook != NULL
    || (_dl_addr (_IO_vtable_check, &di, &l, NULL) != 0
        && l->l_ns != LM_ID_BASE))
  return;
```

Vtable verification

- Summary of the vtable verification
  - It very hard to bypass it.
  - Exploitation of FILE structure is dead ?

Vtable verification

- Summary of the vtable verification
  - It very hard to bypass it.
  - Exploitation of FILE structure is dead ?
    - No

Agenda

- Introduction
  - File stream
  - Overview the FILE structure
- Exploitation of FILE structure
  - FSOP
  - Vtable verification in FILE structure
  - Make FILE structure great again
- Conclusion

Make FILE structure great again

- How about change the target from vtable to other element ?
  - Stream Buffer & File Descriptor

```
struct _IO_FILE {
  int _flags;       /* f
  char* _IO_read_ptr;
  char* _IO_read_end;
  char* _IO_read_base;
  char* _IO_write_base;
  char* _IO_write_ptr;
  char* _IO_write_end;
  char* _IO_buf_base;
  char* _IO_buf_end;
  int _fileno;
  ...
  char _shortbuf[1];
  ...
};
```

Make FILE structure great again

- If we can overwrite the FILE structure and use fread and fwrite with the FILE structure
  - We can
    - Arbitrary memory reading
    - Arbitrary memory writing

Make FILE structure great again

- Arbitrary memory reading
  - fwrite
    - Set the _fileno to the file descriptor of stdout
    - Set _flag & ~_IO_NO_WRITES
    - Set _flag |= _IO_CURRENTLY_PUTTING
    - Set the write_base & write_ptr to memory address which you want to read
    - Set _IO_read_end equal to _IO_write_base

Make FILE structure great again

- Arbitrary memory reading
  - Set _flag &~ _IO_NO_WRITES
  - Set _flag |= _IO_CURRENTLY_PUTTING

```
if (f->_flags & _IO_NO_WRITES) /* SET ERROR */
      return EOF
if ((f->_flags & _IO_CURRENTLY_PUTTING) == 0 || f->_IO_write_base == NULL)
  {
      ...
  }
if (ch == EOF)
  return _IO_do_write (f, f->_IO_write_base,
            f->_IO_write_ptr - f->_IO_write_base);
  ...
}
```

It will adjust the stream buffer

A piece of code in fwrite

Our goal

Make FILE structure great again

- Arbitrary memory reading
  - Let _IO_read_end equal to _IO_write_base
    - If it’s not, it would adjust to the current offset.

```
_IO_size_t count;
if (fp->_flags & _IO_IS_APPENDING)
  ...
else if (fp->_IO_read_end != fp->_IO_write_base)
  {
      ...
  }
count = _IO_SYSWRITE (fp, data, to_do);
  ...
return count;
```

It will adjust the stream buffer

Our goal

Make FILE structure great again

- Arbitrary memory reading
  - Sample code

```
char *msg = "secret";
FILE *fp;
char *buf = malloc(100);
read(0,buf,100);
fp = fopen("key.txt","rw");
```

```
fwrite(buf,1,100,fp);
```

Make FILE structure great again

- Arbitrary memory reading
  - Sample code

```
char *msg = "secret";
FILE *fp;
char *buf = malloc(100);
read(0,buf,100);
fp = fopen("key.txt","rw");
fp->_flags &= ~8;
fp->_flags |= 0x800 ;
fp->_flags |= _IO_IS_APPENDING ;
fp->_IO_write_base = msg;
fp->_IO_write_ptr = msg+6;
fp->_IO_read_end = fp->_IO_write_base;
fp->_fileno = 1;

fwrite(buf,1,100,fp);
```

```
angelboy@ubuntu:~/cmt$ ./arbitrary_read
hello
secrethello
```

Make FILE structure great again

- Arbitrary memory writing
  - fread
    - Set the _fileno to file descriptor of stdin
    - Set _flag &~ _IO_NO_READS
    - Set read_base equals to read_ptr
    - Set the buf_base & buf_end to memory address which you want to wirte
    - buf_end - buf_base > size of fread

Make FILE structure great again

- Arbitrary memory writing
  - Set read_base equal to read_ptr

It will copy data from buffer to destination

```
have = fp->_IO_read_end - fp->_IO_read_ptr;
if (want <= have)
  ...
if (fp->_IO_buf_base
    && want < (size_t) (fp->_IO_buf_end - fp->_IO_buf_base))
{
    if (__underflow (fp) == EOF)
      ...
}
```

Buffer size must be larger than read size

Make FILE structure great again

- Arbitrary memory writing
  - Set _flag &~ _IO_NO_READS

```
if (fp->_flags & _IO_NO_READS)
  {
    return EOF;
  }
  ...
count = _IO_SYSREAD (fp, fp->_IO_buf_base,
                     fp->_IO_buf_end - fp->_IO_buf_base);
```

Our goal

Make FILE structure great again

- Arbitrary memory writing
  - Sample code

```
FILE *fp;
char *buf = malloc(100);
char msg[100];
fp = fopen("key.txt","rw");
```

```
fread(buf,1,6,fp);
puts(msg);
```

Make FILE structure great again

- Arbitrary memory writing
  - Sample code

```
FILE *fp;
char *buf = malloc(100);
char msg[100];
fp = fopen("key.txt","rw");
fp->_flags &= ~4;
fp->_IO_buf_base = msg;
fp->_IO_buf_end = msg+100;
fp->_fileno = 0;
fread(buf,1,6,fp);
puts(msg);
```

```
angelboy@ubuntu:~/cmt$ ./arbitrary_write
hi hitb
hi hitb
```

Make FILE structure great again

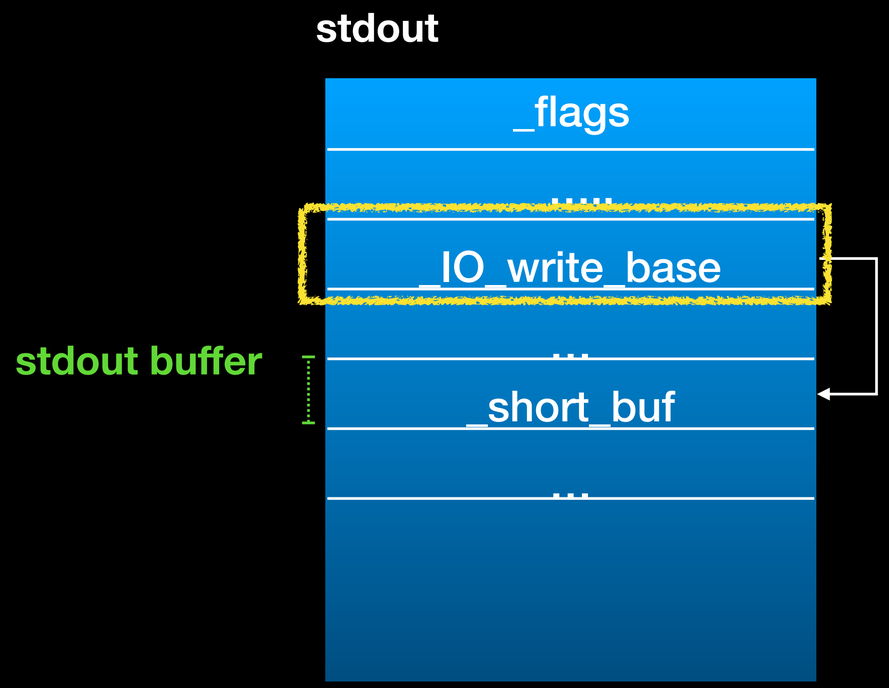
- If you have arbitrary memory address read and write, you can control the flow very easy
  - GOT hijack
  - __malloc_hook_/__free_hook_/__realloc_hook_
  - …
- By the way, you can not only use fread and fwrite but also use any I/O related function

Make FILE structure great again

- If we don’t have any file operation in the program
  - We can use stdin/stdout/stderr
    - put/printf/scanf
    - …

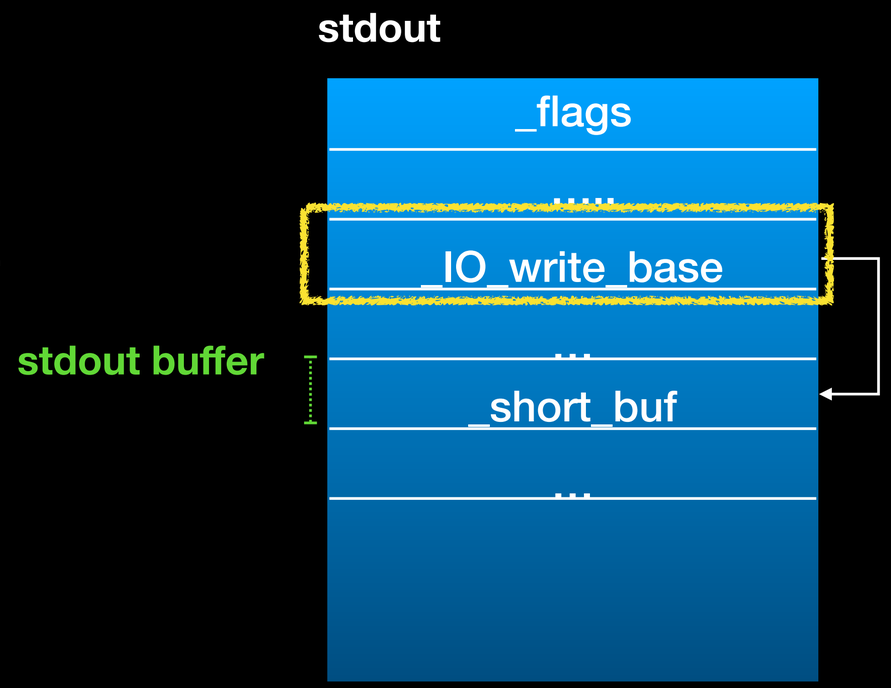
Make FILE structure great again

- Scenario - information leak
  - Use any stdout related function
    - printf/fputs/puts ...



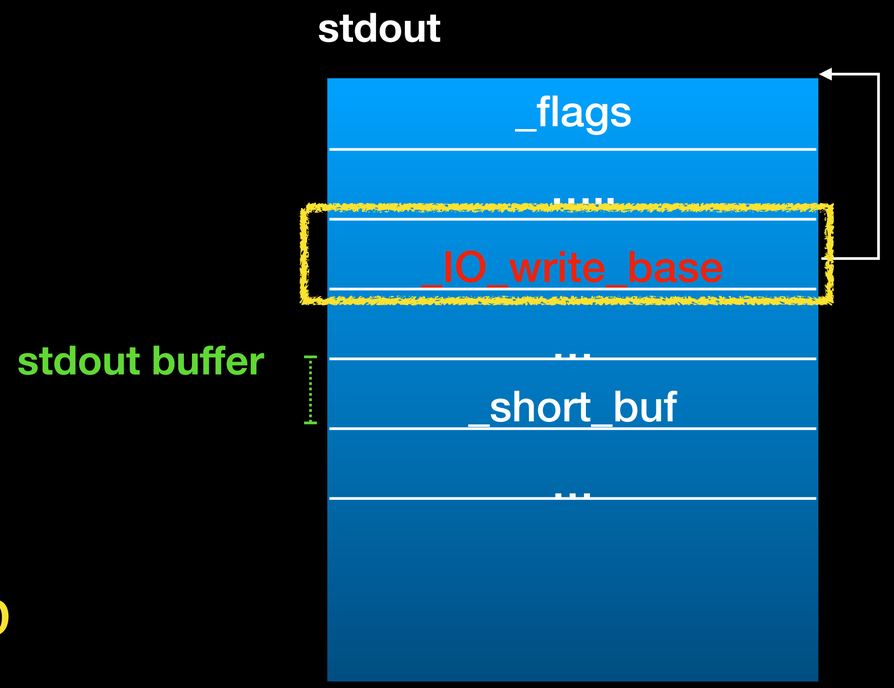
Make FILE structure great again

- Overwrite _flags and partial overwrite _IO_write_base pointer
  - Fastbin attack
    - Partial overwrite unsorted bin pointer
    - Very like House of Roman



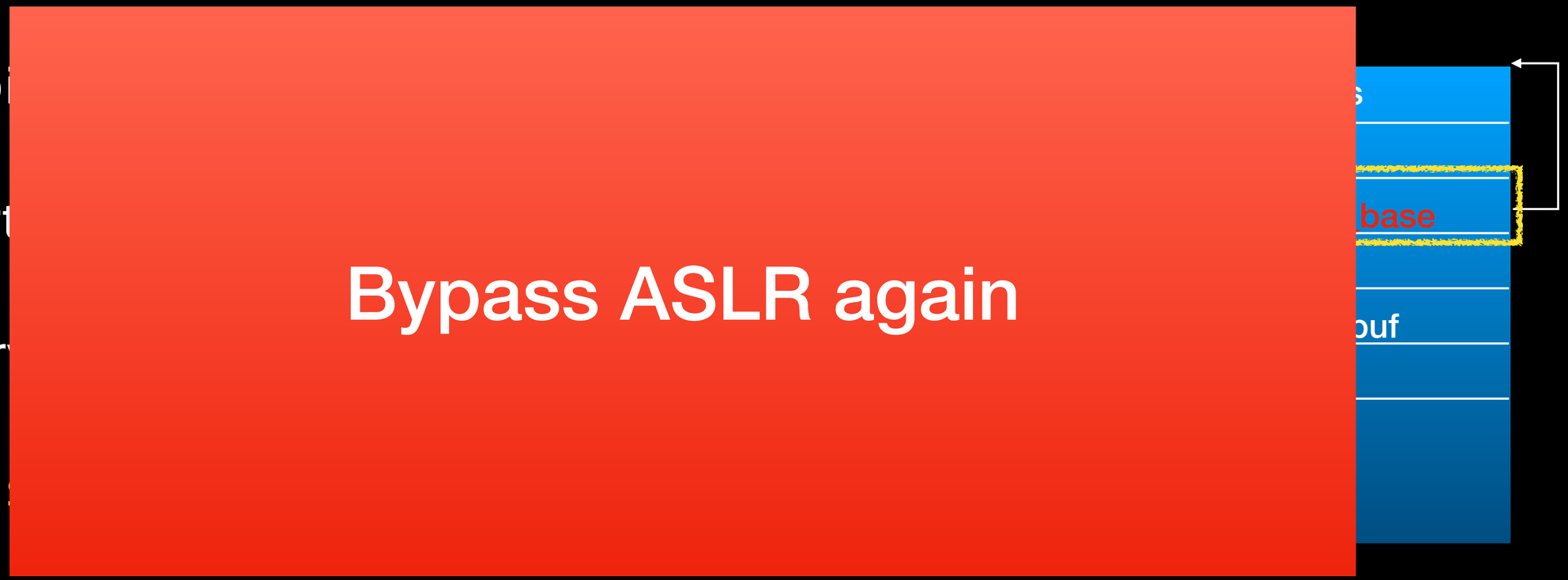
Make FILE structure great again

- Overwrite _flags and partial overwrite _IO_write_base pointer
  - Fastbin attack
    - Partial overwrite unsorted bin pointer
    - Very like House of Roman
  - Leak some memory data in libc or heap



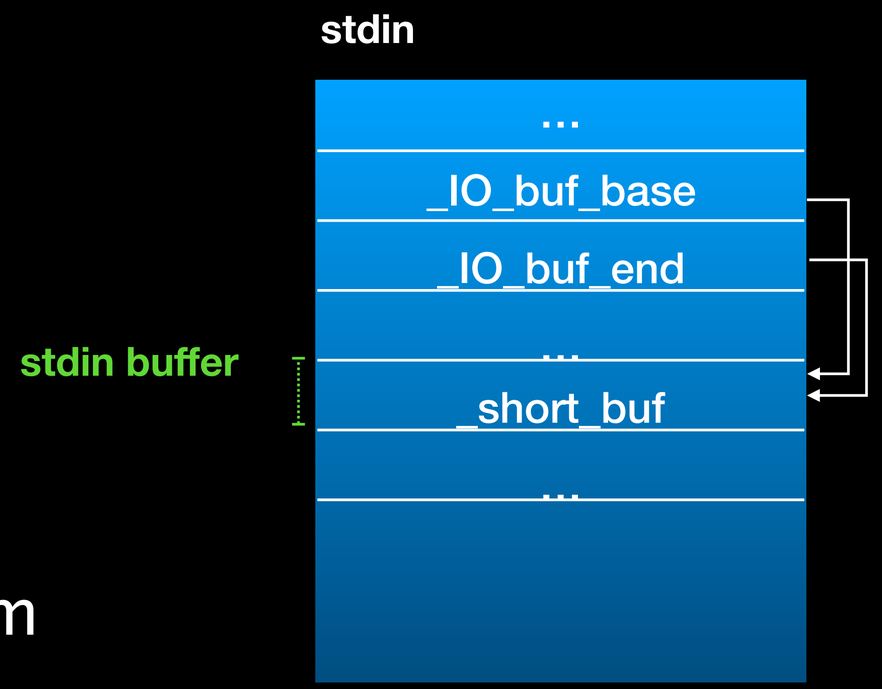
Make FILE structure great again

- Overwrite _flags and partial overwrite _IO_write_base pointer
  - Fastbi
    - Part
    - Ver
  - Leak



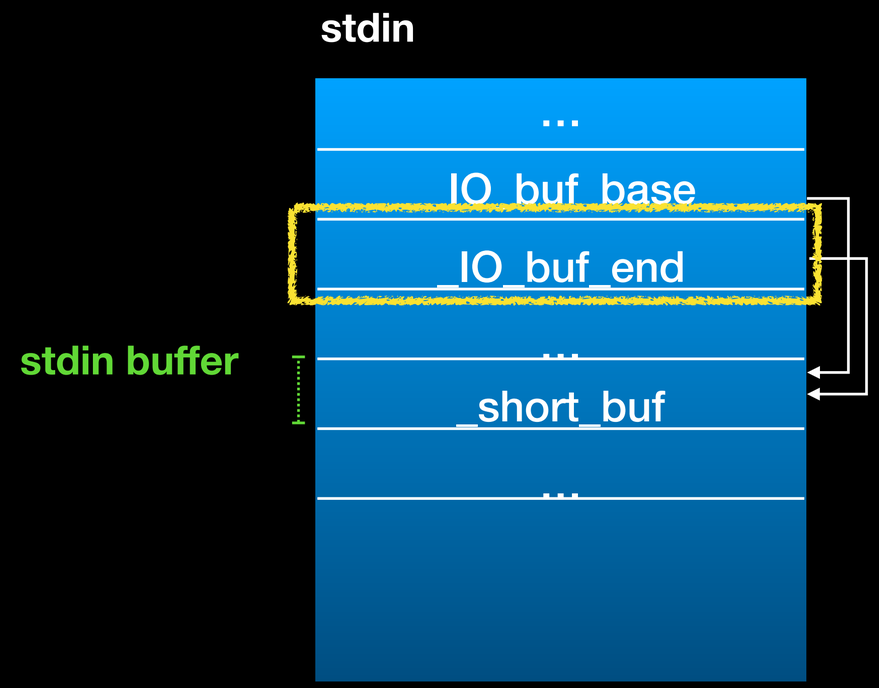
Make FILE structure great again

- Scenario - Code execution
  - Use any stdin related function
    - scanf/fgets/gets ...
  - Stdin is unbuffer
    - Very common in normal stdio program



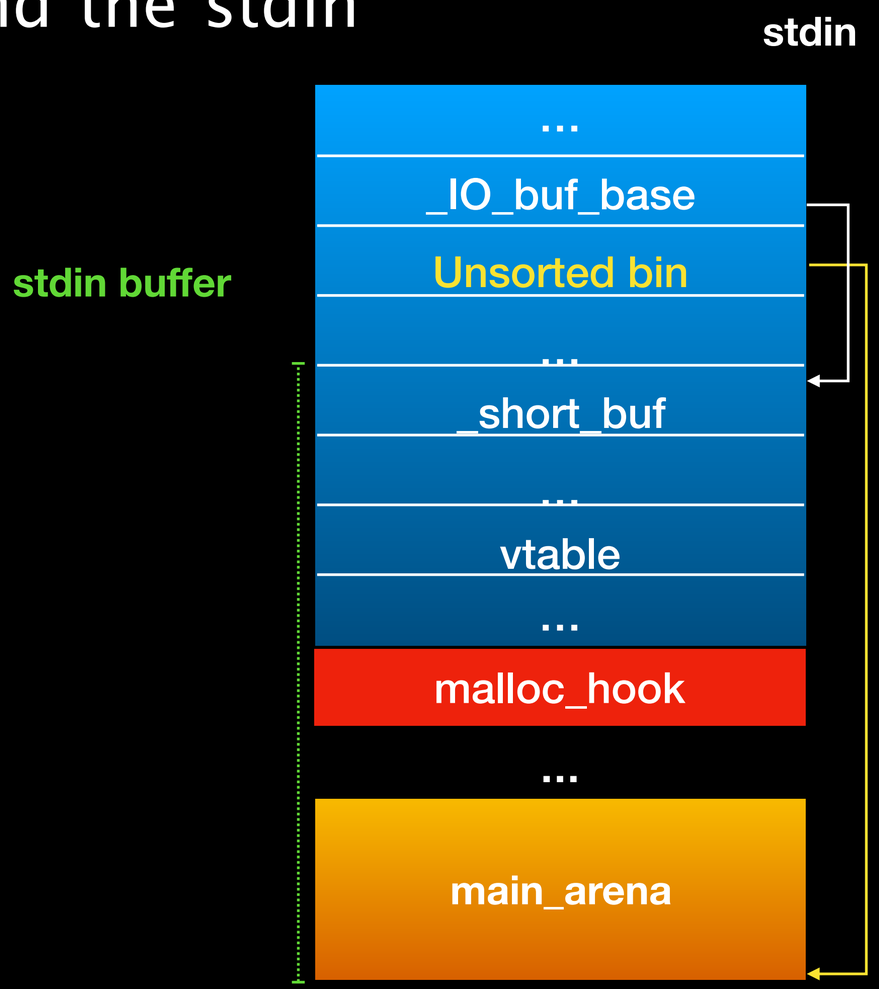
Make FILE structure great again

- Overwrite buf_end with a pointer behind the stdin
  - Unsorted bin attack
    - Very common in heap exploitation



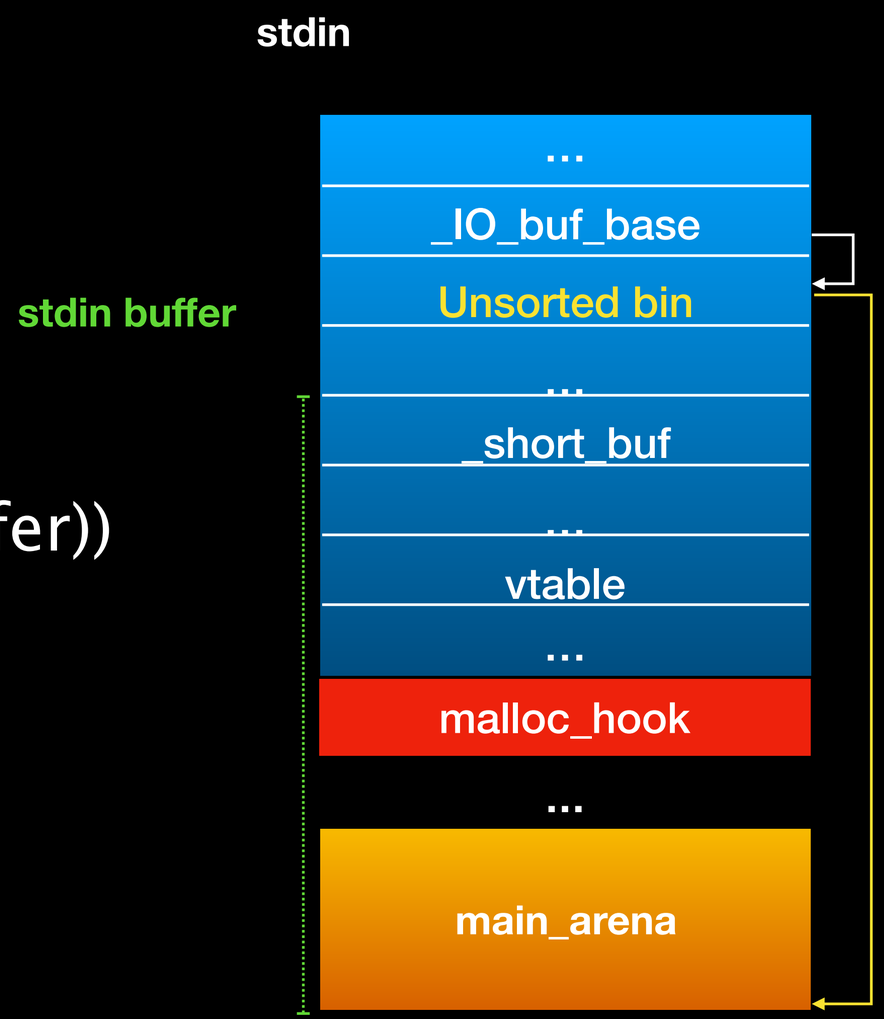
Make FILE structure great again

- Overwrite buf_end with a pointer behind the stdin
  - Unsorted bin attack
    - Very common in heap exploitation



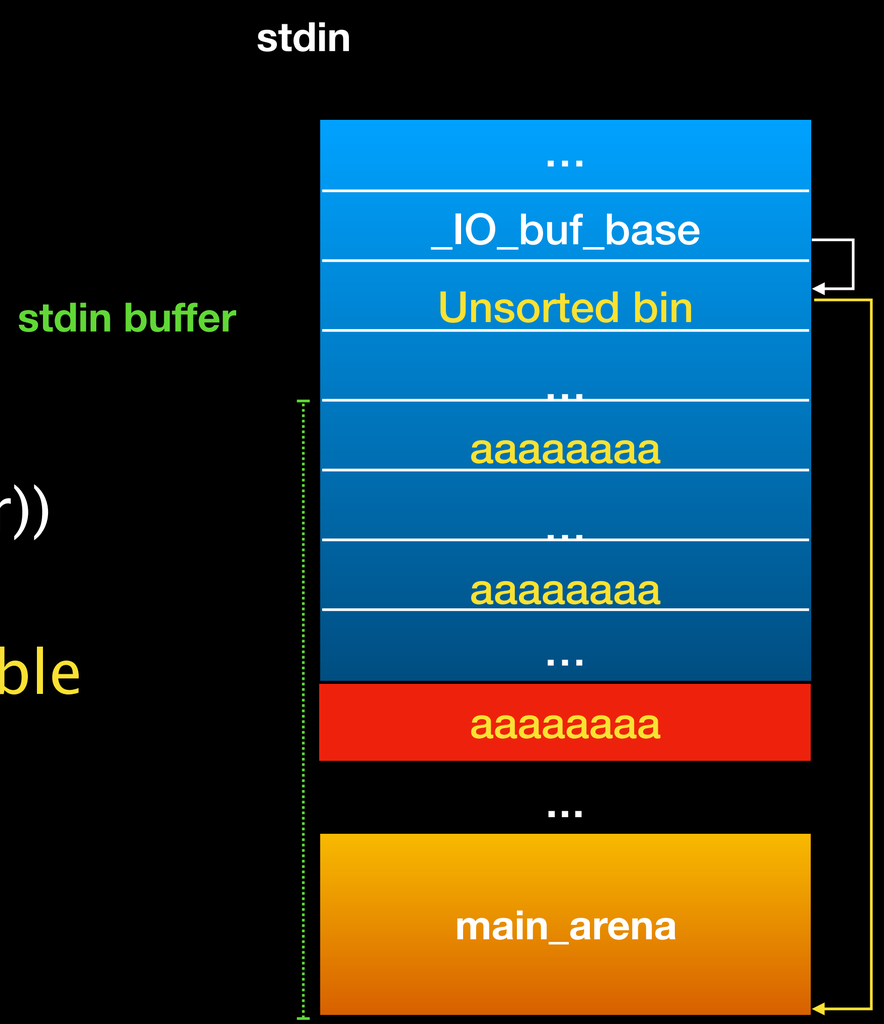
Make FILE structure great again

- Stdin related function
  - scanf(“%d”,&var)
    - It will call
      - read(0,buf_base,sizeof(stdin buffer))



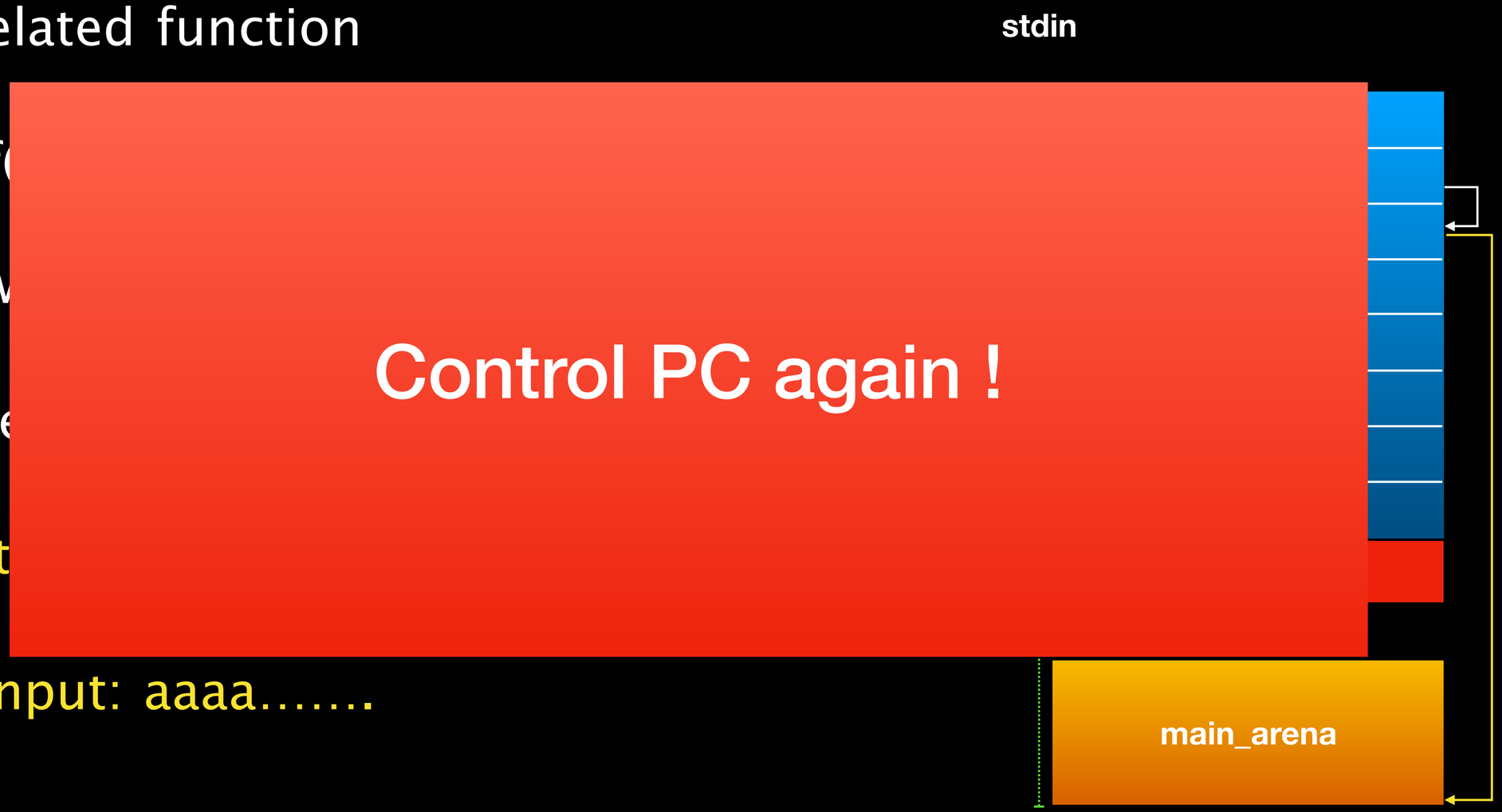
Make FILE structure great again

- Stdin related function
  - scanf(“%d”,&var)
    - It will call
      - read(0,buf_base,sizeof(stdin buffer))
      - It can overwrite many global variable in glibc
      - Input: aaaa……



Make FILE structure great again

- Stdin related function
  - scanf(
    - It w
      - re
      - It
      - Input: aaaa.....



Make FILE structure great again

- Another bypass method
  - Use existing function in the validated function which use _IO_strfile structure

```
38 struct _IO_streambuf
39 {
40   struct _IO_FILE _f;
41   const struct _IO_jump_t *vtable;
42 };
43
44 typedef struct _IO_strfile_
45 {
46   struct _IO_streambuf _sbf;
47   struct _IO_str_fields _s;
48 } _IO_strfile;
```

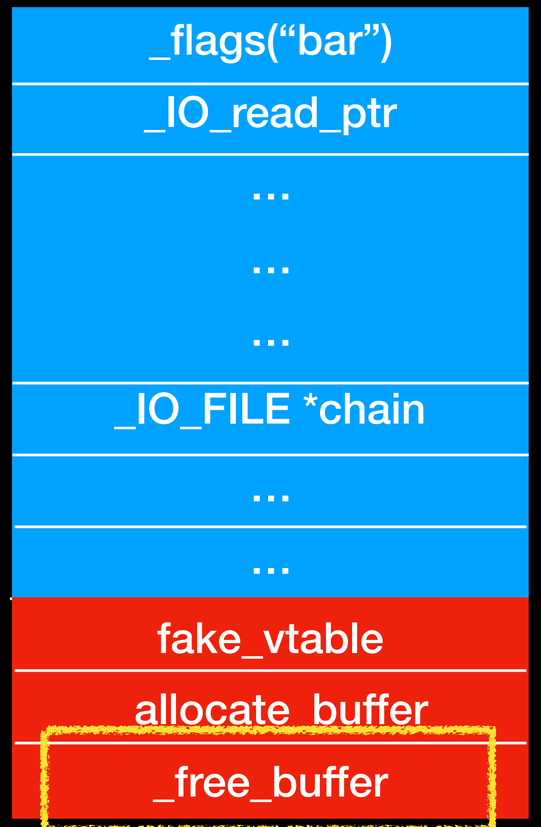
```
29 typedef void *(*_IO_alloc_type) (_IO_size_t);
30 typedef void (*_IO_free_type) (void*);
31
32 struct _IO_str_fields
33 {
34   _IO_alloc_type _allocate_buffer;
35   _IO_free_type _free_buffer;
36 };
```

No vtable check

Make FILE structure great again

- Another bypass method
  - Use existing function in the validated function which use _IO_strfile structure

```
345 void
346 _IO_str_finish (_IO_FILE *fp, int dummy)
347 {
348   if (fp->_IO_buf_base && !(fp->_flags & _IO_USER_BUF))
349     (((_IO_strfile *) fp)->_s._free_buffer) (fp->_IO_buf_base);
350   fp->_IO_buf_base = NULL;
351
352   _IO_default_finish (fp, 0);
353 }
```



Function pointer

Make FILE structure great again

- Another bypass method
  - Use existing function in the validated function which use _IO_strfile structure
    - _IO_str_jumps
      - https://dhavalkapil.com/blogs/FILE-Structure-Exploitation/
    - _IO_wstr_finish
      - https://tradahacking.vn/hitcon-2017-ghost-in-the-heap-writeup-ee6384cd0b7
    - _IO_str_finish

    ...

Lab 12-4

- The return of see the file

Make FILE structure great again

- How about Windows ?

Make FILE structure great again

- How about Windows ?
  - No vtable in FILE

```
121 struct __crt_stdio_stream_data
122 {
123     union
124     {
125         FILE  _public_file;
126         char* _ptr;
127     };
128
129     char*            _base;
130     int              _cnt;
131     long             _flags;
132     long             _file;
133     int              _charbuf;
134     int              _bufsiz;
135     char*            _tmpfname;
136     CRITICAL_SECTION _lock;
137 };
138
```

Make FILE structure great again

- How about Windows ?
  - No vtable in FILE
  - It also has stream buffer pointer
    - You can corrupt it to achieve arbitrary memory reading and writing

Agenda

- Introduction
  - File stream
  - Overview the FILE structure
- Exploitation of FILE structure
  - FSOP
  - Vtable verification in FILE structure
  - Make FILE structure great again
- Conclusion

Conclusion

- FILE structure is a good target for binary exploitation
  - It can be used to
    - Arbitrary memory read and write
    - Control the PC and do oriented programing
    - Other exploit technology
      - Arbitrary free/unmmap
      - …

Conclusion

- FILE structure is a good target for binary Exploit
  - It’s very powerful in some unexploitable case

HW 0xc

- Heap paridise

Thank you for listening

Mail : angelboy@chroot.org

Blog : blog.angelboy.tw

Twitter : @scwuaptx