Exceptional Control Flow: Exceptions and Processes

CSE4009: System Programming

Woong Sul

Today

- Exceptional Control Flow
- Exceptions
- Processes
- Process Control

Control Flow → 프로그램 코드에 표현된 기본 실행 흐름

- Processors do only one thing:
  - From startup to shutdown, a CPU simply reads and executes (interprets) a sequence of instructions, one at a time
  - This sequence is the CPU's control flow (or flow of control)

(Physical) control flow

Time

<startup>

$inst_1$

$inst_2$

$inst_3$

…

$inst_n$

<shutdown>

Altering the Control Flow

- Up to now: two mechanisms for changing control flow:
  - Jumps and branches
  - Call and return

  ➔ React to changes in ***program state***

- Insufficient for a useful system:
  Difficult to react to changes in ***system state***
  - Data arrives from a disk or a network adapter
  - Instruction divides by zero
  - User hits Ctrl-C at the keyboard
  - System timer expires

- System needs mechanisms for “Exceptional Control Flow”

Exceptional Control Flow

- Exists at all levels of a computer system
- Low level mechanisms

1. **Exceptions** Interupt
   - Change in control flow in response to a system event (i.e., change in system state)
   - Implemented using combination of hardware and OS software

- Higher level mechanisms

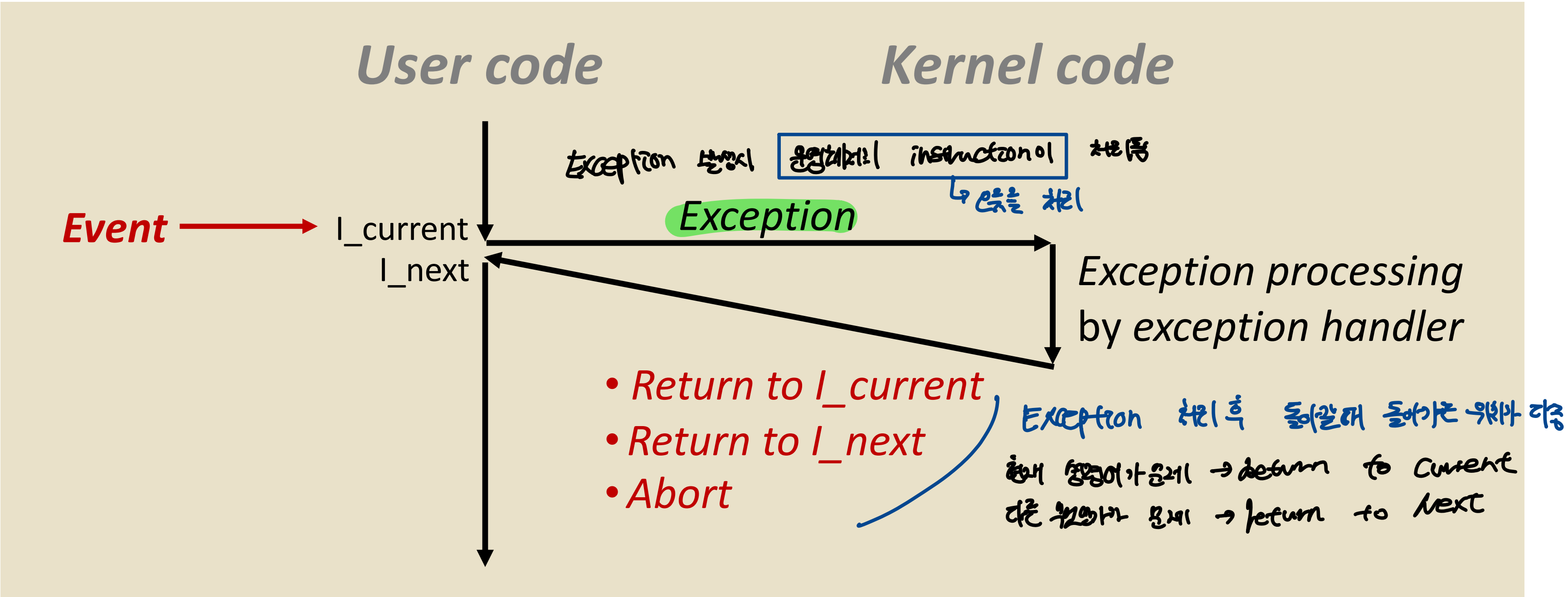
2. **Process context switch**
   - Implemented by OS software and hardware timer
3. **Signals**
   - Implemented by OS software

Today

- Exceptional Control Flow
- Exceptions
- Processes
- Process Control

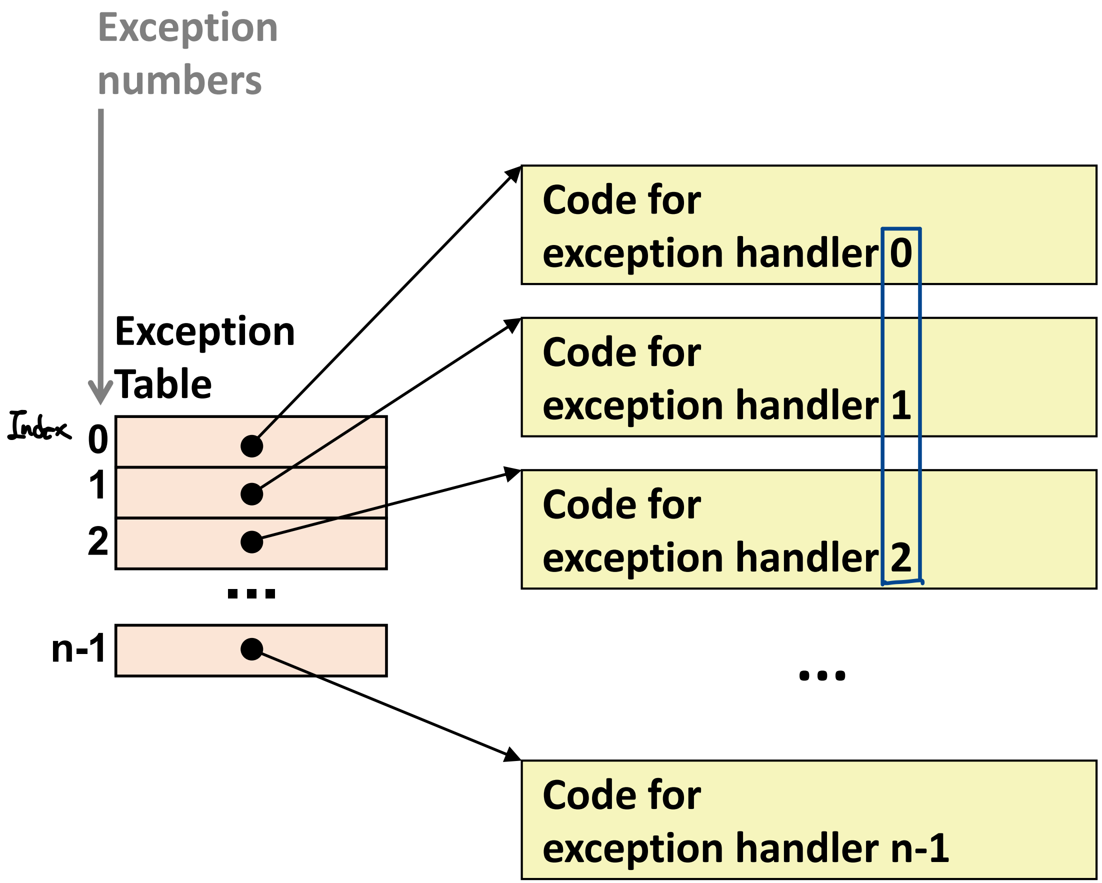
Exceptions

- An ***exception*** is a transfer of control to the OS kernel in response to some *event* (i.e., change in processor state)
  - Kernel is the memory-resident part of the OS
  - Examples of events: Divide by 0, arithmetic overflow, page fault, I/O request completes, typing Ctrl-C



Exception Tables

- Exception handlers might be implemented by SW



- Each type of event has a unique exception number k
- k = index into exception table (a.k.a. interrupt vector)
- Handler k is called each time exception k occurs

- How to call the handler?
  - i.e., How does packet arrival interrupt the current flow

Asynchronous Exceptions (Interrupts)

비동기화

외부 요소에 의한 것

- Caused by events external to the processor
  - Indicated by setting the processor's ***interrupt pin***
  - Handler returns to $\boxed{\text{“next”}}$ instruction

Interrupt pin을 set

비동기화
→ Global Time에 대해
process와 external의
선후관계가 정해져있지 않았다.

- Examples:
  - Timer interrupt
    - Every few ms, an external timer chip triggers an interrupt
    - Used by the kernel to take back control from user programs
  - I/O interrupt from external device
    - Hitting Ctrl-C at the keyboard
    - Arrival of a packet from a network
    - Arrival of data from a disk

Synchronous Exceptions

Instruction:(종류

- Caused by events that occur as a result of executing an instruction: → Process 내에서
  - ***Traps***
    - Intentional ➔ like procedure calls → 문제가 있는 것이 아닌 의도적으로 Control Flow를 변화시킨 것
    - Examples: ***system calls***, breakpoint traps, special instructions
    - Returns control to "next" instruction
  - ***Faults***
    - Unintentional but possibly recoverable
    - Examples: page faults (recoverable), protection faults (unrecoverable), floating point exceptions
    - Either re-executes faulting ("current") instruction or aborts
  - ***Aborts***
    - Unintentional and unrecoverable
    - Examples: illegal instruction, parity error, machine check
    - Aborts current program → 복구 불가능이므로 실행 자체를 종료

System Calls

library 함수는 System call을 실행한다.

- Each x86-64 system call has a unique ID number
- Examples:

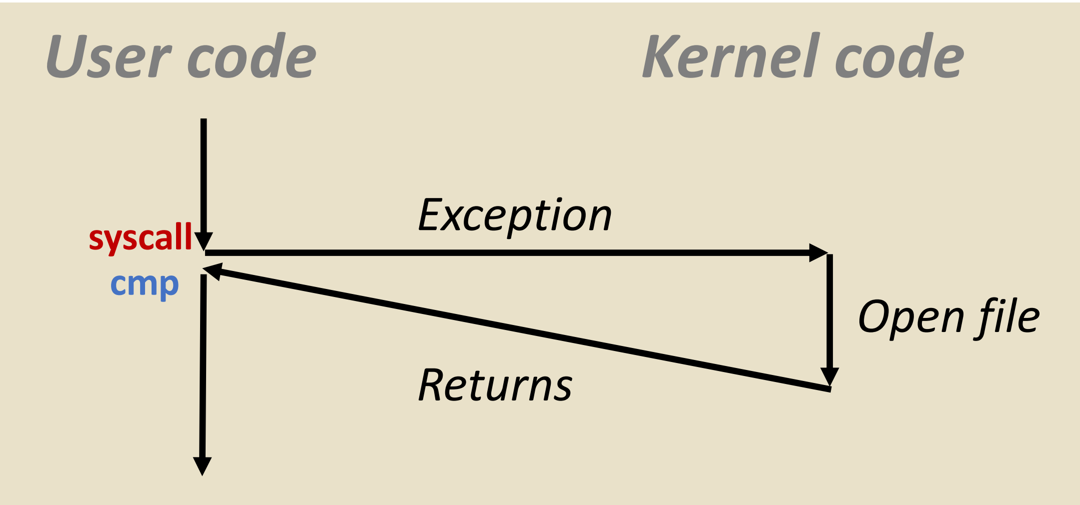
Example of TRAP

Number	*Name*	*Description*
0	`read`	Read file
1	`write`	Write file
2	`open`	Open file
3	`close`	Close file
4	`stat`	Get info about file
57	`fork`	Create process
59	`execve`	Execute a program
60	`_exit`	Terminate process
62	`kill`	Send signal to process

System Call Example: Opening File

- User calls: `open(filename, options)`
- Calls `__open()`, which invokes system call `syscall`

```
00000000000e5d70 <__open>:
...
e5d79:   b8 02 00 00 00        mov   $0x2,%eax   # open is syscall #2
e5d7e:   0f 05                 syscall           # Return value in %rax
e5d80:   48 3d 01 f0 ff ff     cmp   $0xfffffffffffff001,%rax
...
e5dfa:   c3                    retq
```



함수의 종류를 저장

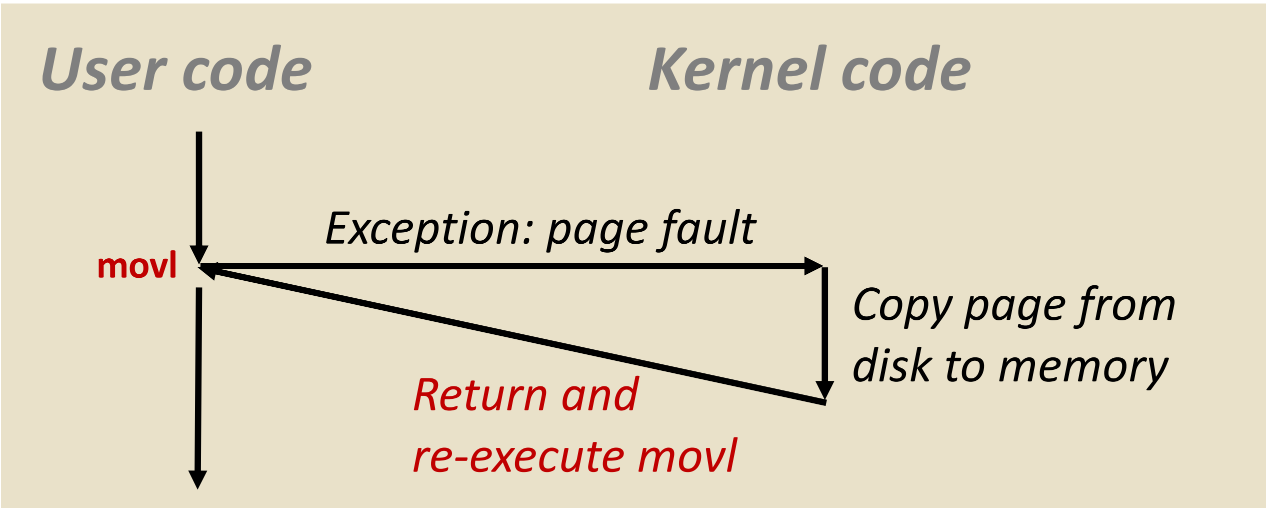
- `%rax` contains syscall number
- Other arguments in `%rdi`, `%rsi`, `%rdx`, `%r10`, `%r8`, `%r9`
- Return value in `%rax`
- Negative value is an error corresponding to negative `errno`
- zero 는 정상

Fault Example: Page Fault

- User writes to memory location
- That portion (page) of user's memory is currently on disk

```
int a[1000];
main ()
{
    a[500] = 13;
}
```

```
80483b7:        c7 05 10 9d 04 08 0d    movl    $0xd,0x8049d10
```



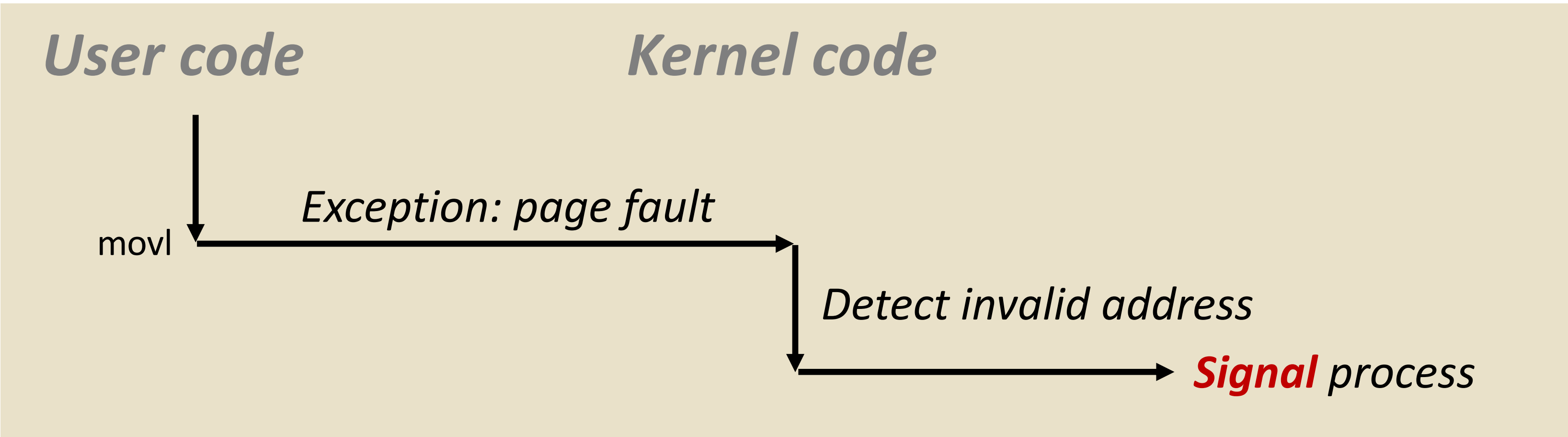
Fault Example: Invalid Memory Reference

- Sends `SIGSEGV` signal to user process
  ↳ 이 시그널을 통해 program을 종료할 수 있도록 함
- User process exits with "segmentation fault"

```
int a[1000];
main ()
{
    a[5000] = 13;
}
```

→ unrecoverable

```
80483b7:     c7 05 60 e3 04 08 0d    movl    $0xd,0x804e360
```



Today

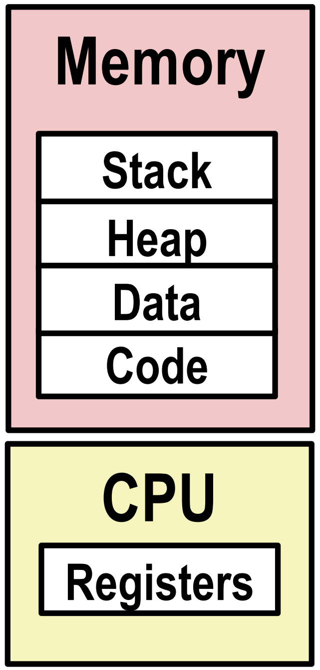
- Exceptional Control Flow
- Exceptions
- Processes
- Process Control

Processes

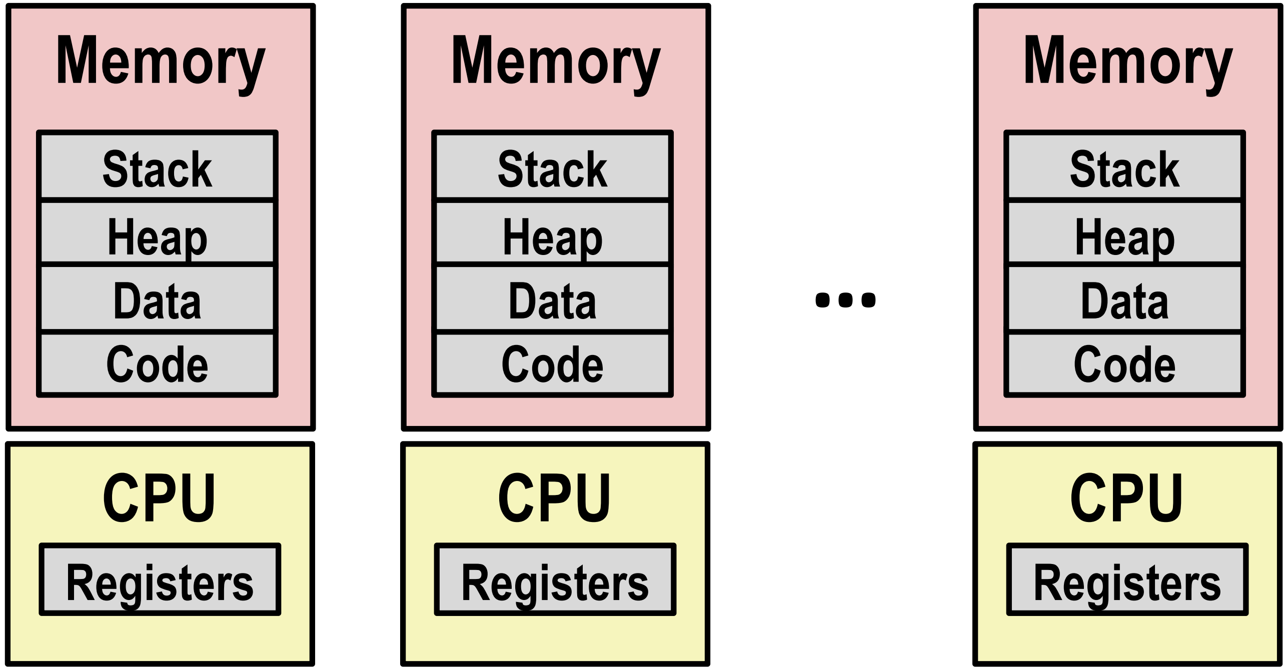
- An instance of a ***running program***
  - One of the most profound ideas in computer science
  - Not the same as “program” or “processor”

각 프로그램이 CPU를 통해 독립적으로 실행되기 위해서 운영체제에서 아래 2가지를 제공

- Process provides each program with two key abstractions:
  - ***Logical control flow*** → 각 process의 CPU 상태 정보(memory)를 저장하도록
    - Each program seems to have exclusive use of the CPU
    - Provided by kernel mechanism called ***context switching***
  - ***Private address space***
    - Each program seems to have exclusive use of main memory
    - Provided by kernel mechanism called ***virtual memory***



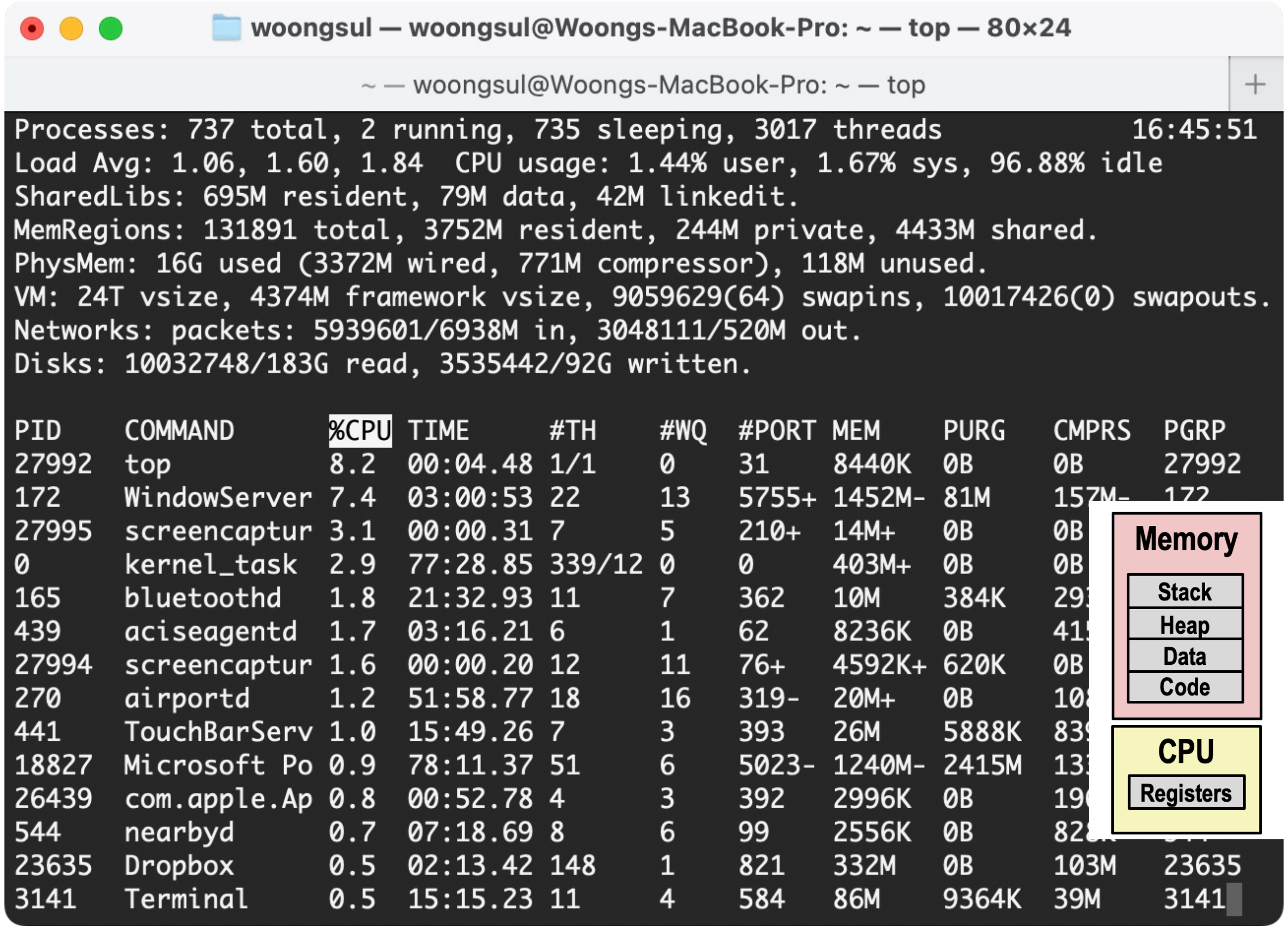
Multiprocessing: The Illusion

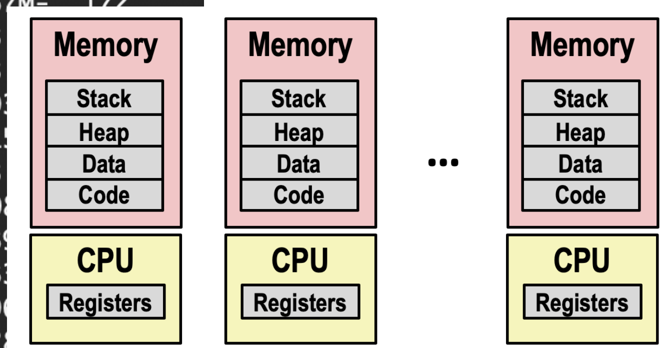


- Computer runs many processes simultaneously
  - Applications for one or more users
    - Web browsers, email clients, editors, …
  - Background tasks
    - Monitoring network & I/O devices

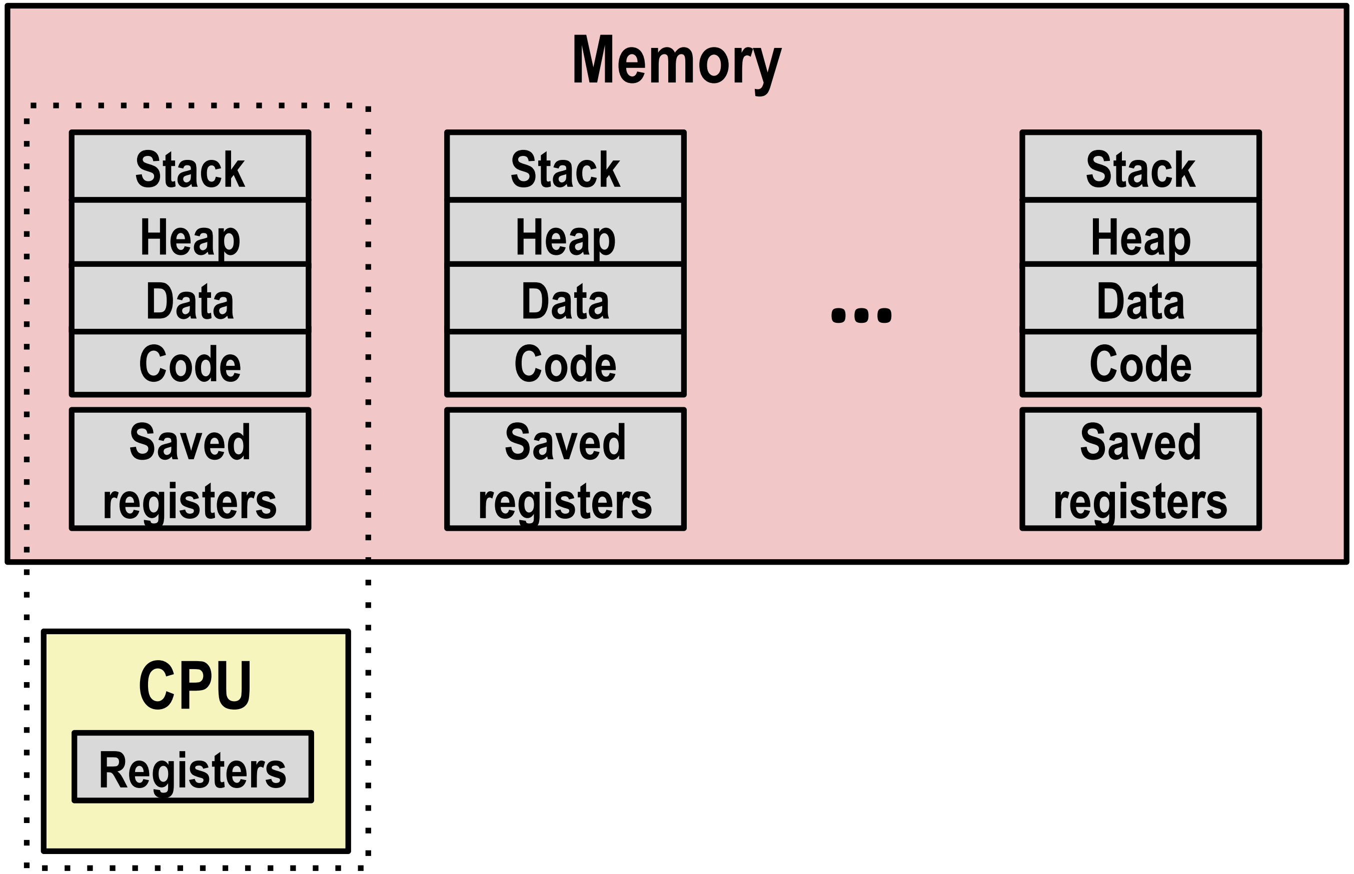
Multiprocessing Example

- Running program "top" on Mac
  - System has 737 processes, 2 of which are active
  - Identified by Process ID (PID)



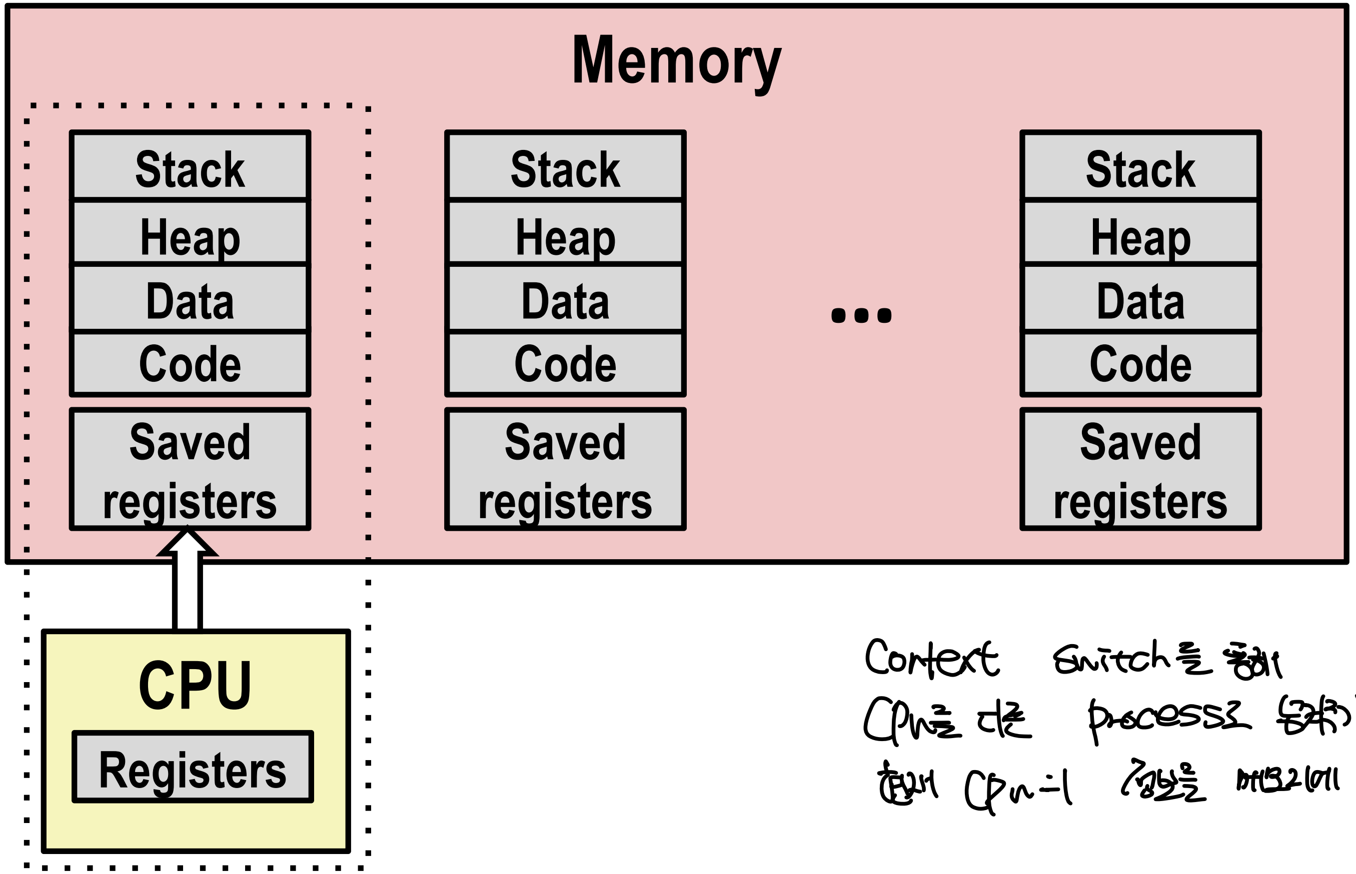


Multiprocessing: The (Traditional) Reality



- Single processor executes multiple processes concurrently
  - Process executions interleaved (multitasking)
  - Address spaces managed by virtual memory system (later in course)
  - Register values for non-executing processes saved in memory

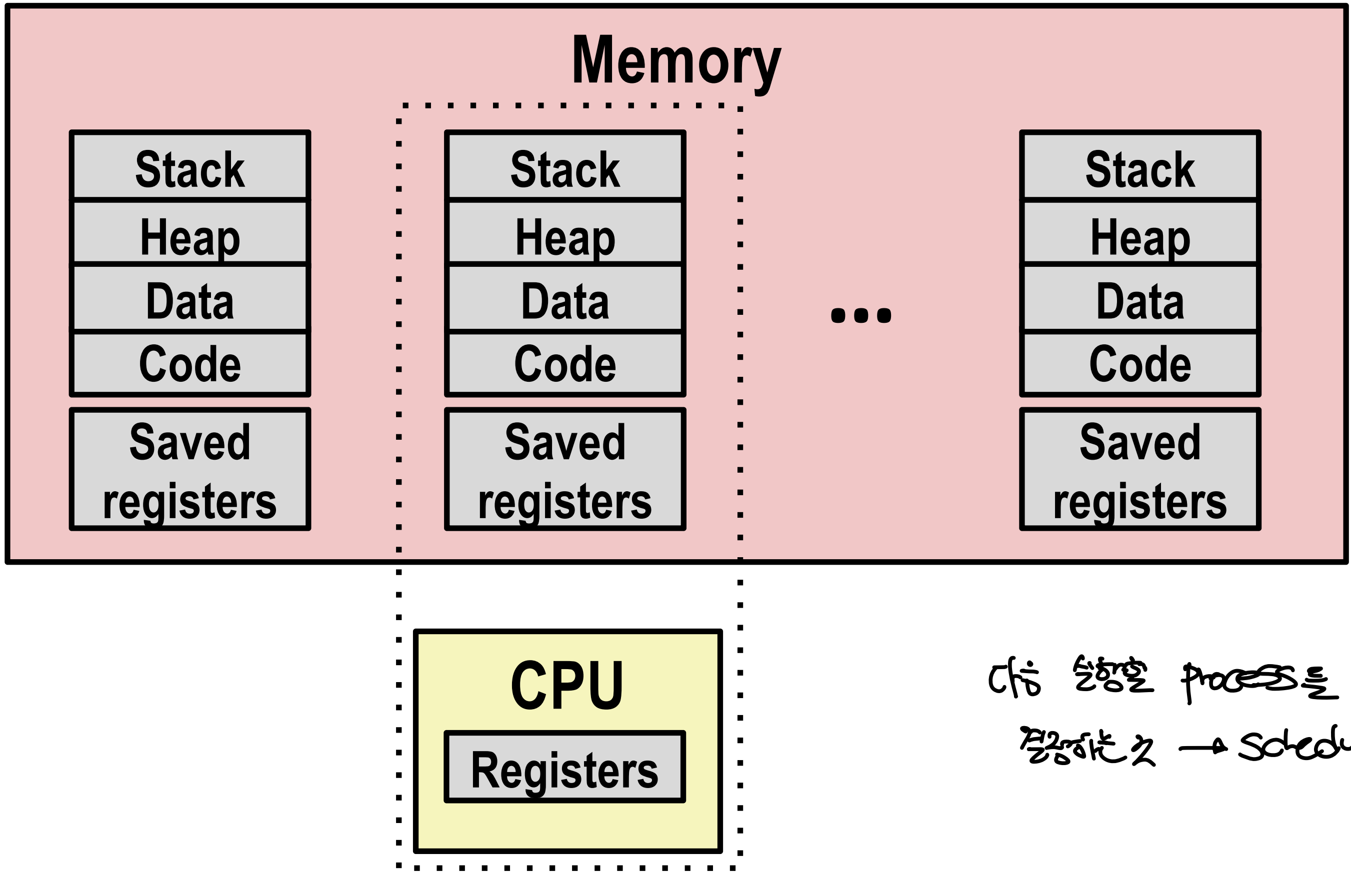
Multiprocessing: The (Traditional) Reality



Context Switch를 통해
Cpu를 다른 process로 넘겨주기전에
현재 Cpu의 정보를 메모리에 저장

- Save current registers in memory

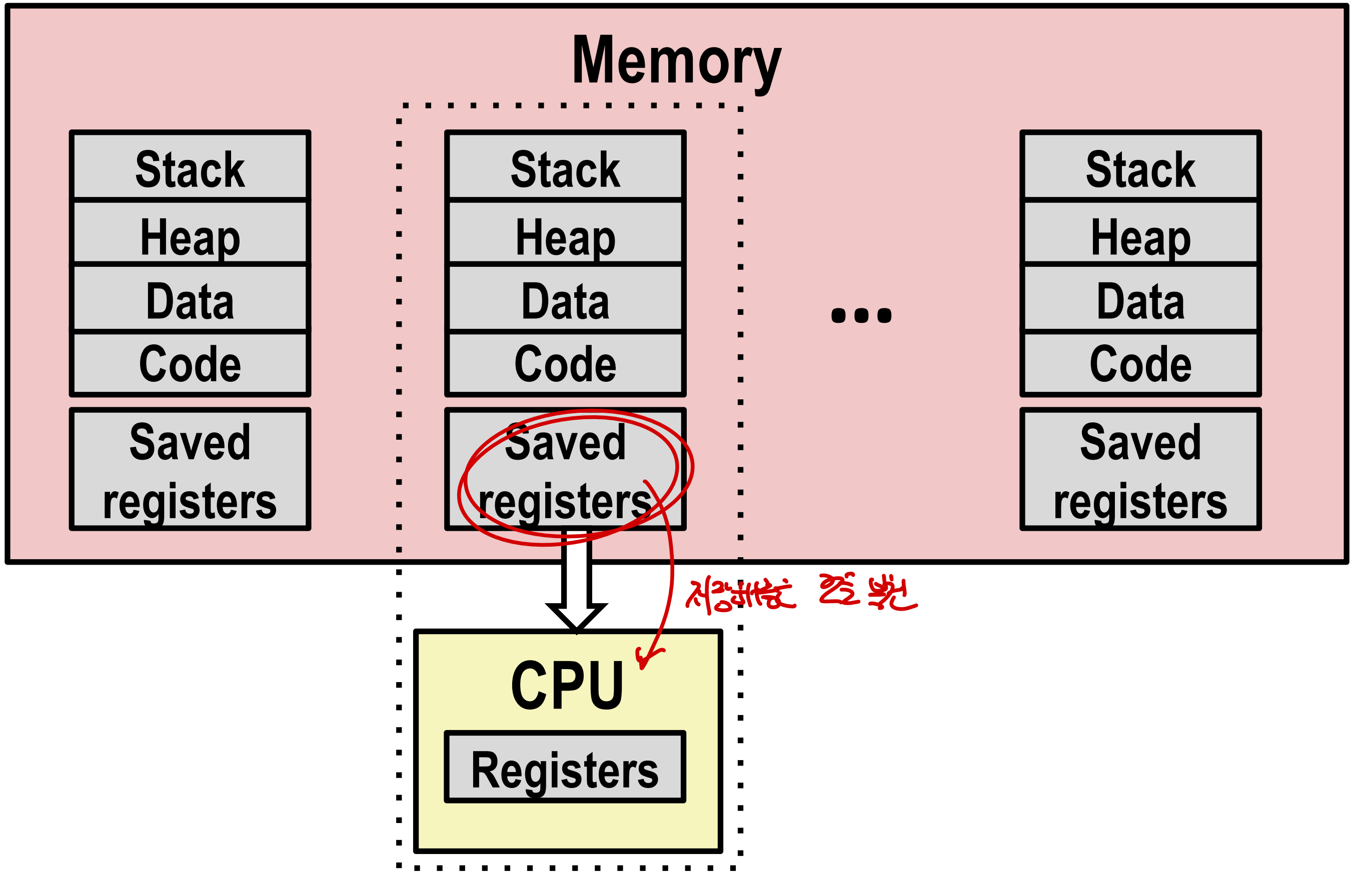
Multiprocessing: The (Traditional) Reality



다음 실행할 process를
결정하는 것 → schedule

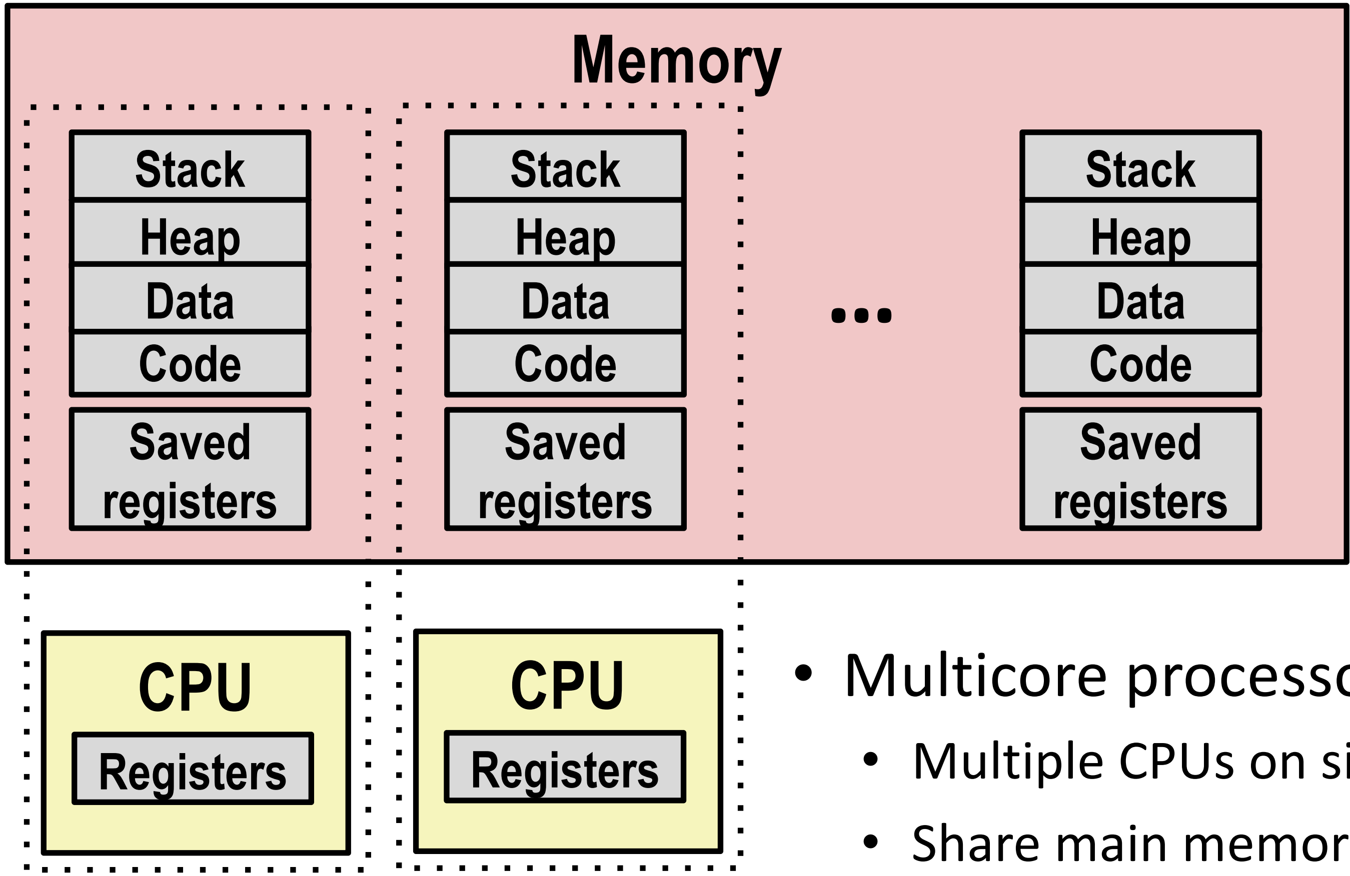
- Schedule next process for execution

Multiprocessing: The (Traditional) Reality



- Load saved registers and switch address space (context switch)

Multiprocessing: The (Modern) Reality



- Multicore processors
  - Multiple CPUs on single chip
  - Share main memory (and some of the caches)
  - Each can execute a separate process
    - Scheduling of processors onto cores done by kernel

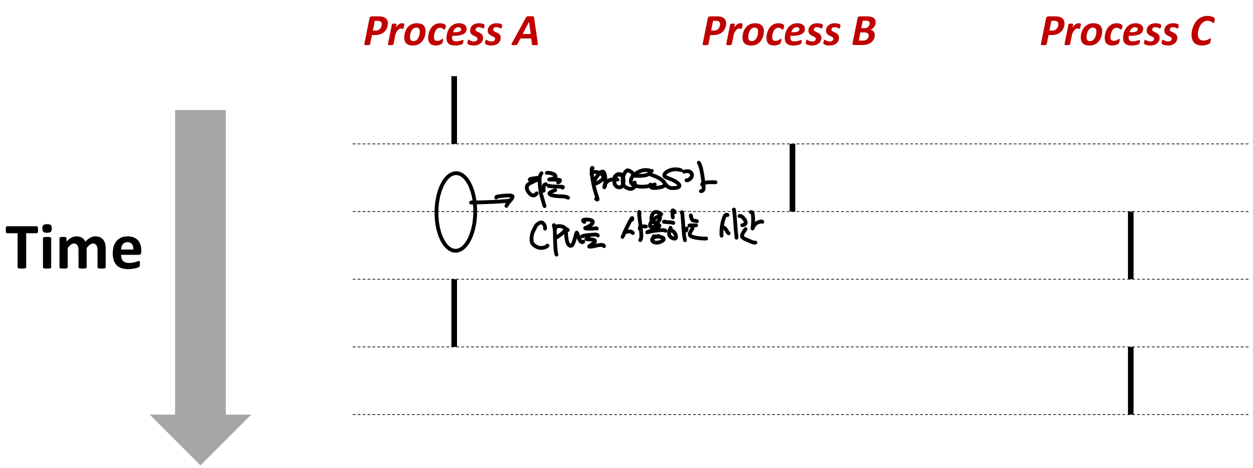
Concurrent Processes

→ 동시에 실행되는 process

- Each process is a logical control flow
- Two processes run ***concurrently*** (are concurrent) if their flows overlap in time
- Otherwise, they are ***sequential***

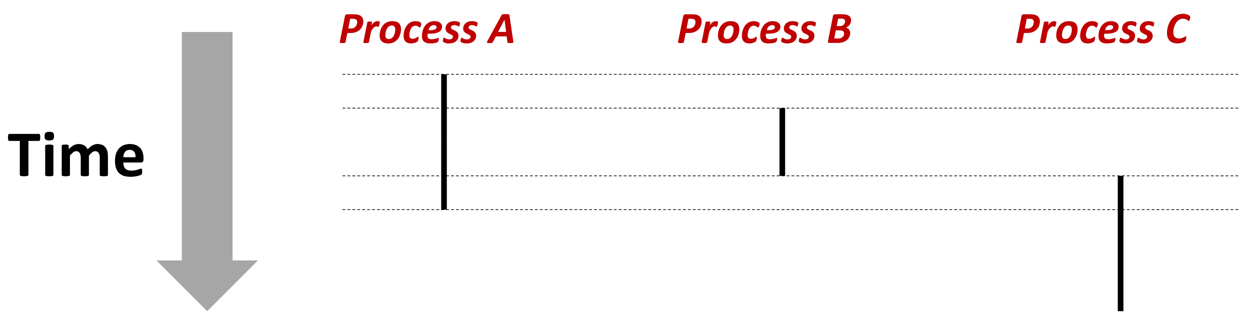
→ 하나의 process가 완전히 종료되고 시작되는 process

- Examples (running on single core):
  - Concurrent: A & B, A & C
  - Sequential: B & C



User View of Concurrent Processes

- Control flows for concurrent processes are ***physically*** disjoint in time
- However, we can think of concurrent processes as ***logically*** running in parallel with each other



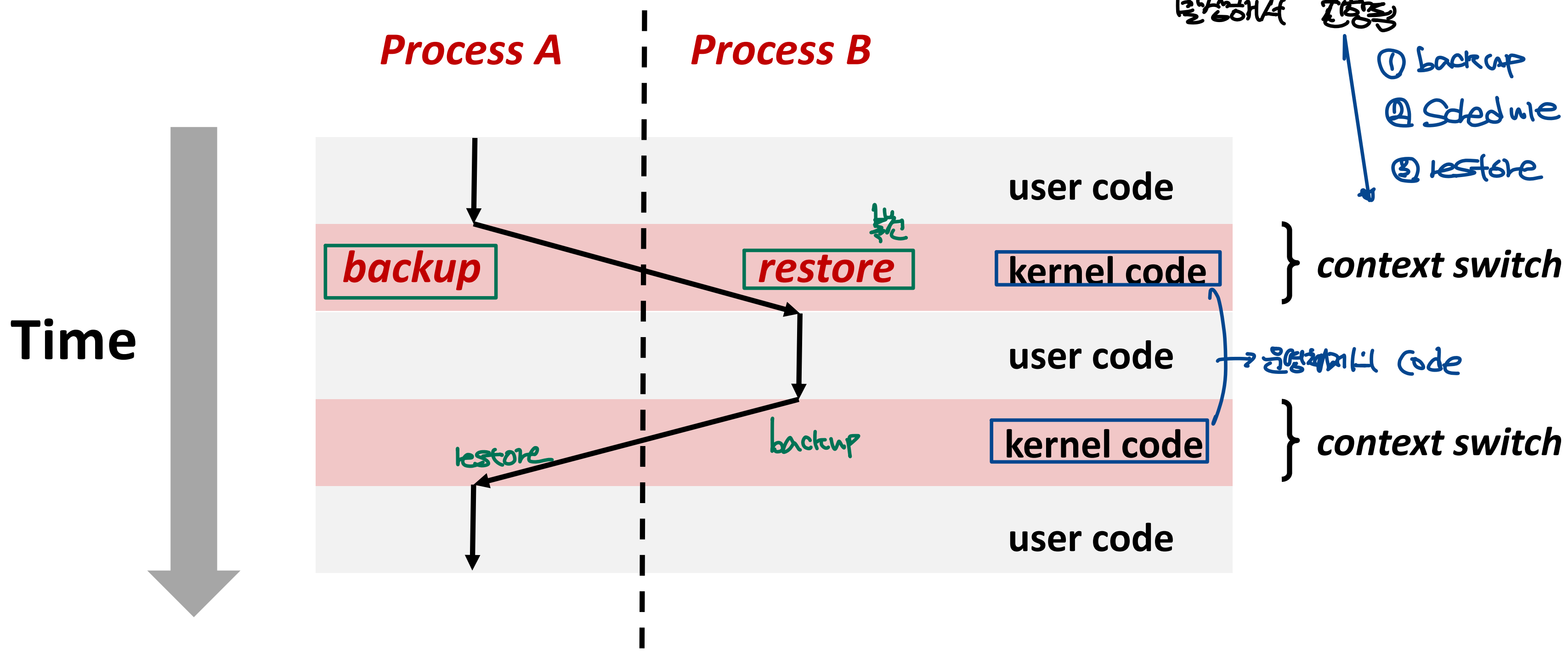
Each process has own logical control flow
but execution time of instructions may vary (why?)

Context Switching

- Processes are managed by a shared chunk of memory-resident OS code called the *kernel*
  - Important: the kernel is not a separate process, but rather runs as part of some existing process
- Control flow passes from one process to another via a *context switch*

timer interrupt에 의해 exception이 발생해서 진행됨

① backup
② schedule
③ restore



Today

- Exceptional Control Flow
- Exceptions
- Processes
- Process Control

System Call Error Handling

- On error, Linux system-level functions typically return -1 and set global variable `errno` to indicate cause

  ↳ 에러의 정보를 담고 있음

- Hard and fast rule:
  - You must check the return status of every system-level function
  - Only exception is the handful of functions that return `void`

- Example:

System call　　　→ error 여부 확인　　　　　　　　　Error message 출력

정수

```
if ((pid = fork()) < 0) {
    fprintf(stderr, "fork error: %s\n", strerror(errno));
    exit(0);
}
```

fork( ) → 자식 process를 만드는 process call

Error-reporting functions

- Can simplify somewhat using an error-reporting function:

```
void unix_error(char *msg) /* Unix-style error */
{
    fprintf(stderr, "%s: %s\n", msg, strerror(errno));
    exit(0);
}
```

```
  if ((pid = fork()) < 0)
     unix_error("fork error");
```

Error-handling Wrappers

- We simplify the code we present to you even further by using Stevens-style error-handling wrappers:

간략화하기 위해 Wrapper function 사용

```
pid_t Fork(void)
{
    pid_t pid;

    if ((pid = fork()) < 0)
        unix_error("Fork error");
    return pid;
}
```

```
  pid = Fork();
```

Obtaining Process IDs

숫자 → process를 구별

- `pid_t getpid(void)`
  - Returns PID of current process

- `pid_t getppid(void)` → 현재 process의 기반이 되는 process
  - Returns PID of parent process

Creating and Terminating Processes

- From a programmer's perspective, we can think of a process as being in one of three states

상태

- Running ← schedule의 대상이 됨
  - Process is either executing, or waiting to be executed and will eventually be ***scheduled*** (i.e., chosen to execute) by the kernel

- Stopped ← process가 종료된 것은 아니지만 당분간 실행될 계획이 없어 schedule의 대상이 안됨
  - Process execution is ***suspended*** and will not be scheduled until further notice (next lecture when we study signals)

- Terminated → process 종료, 명령어를 통해 명시적으로 process를 제거한 상태는 아니다.
  - Process is stopped permanently

→ 바로 삭제되지 않은 이유는 부모 process가 자식 process의 정보를 확인할 수 있도록 하기 위해서

Terminating Processes

- Process becomes terminated for one of three reasons:
  - Returning from the `main` routine
  - Calling the `exit` function
  - Receiving a signal whose default action is to terminate (next lecture)

- `void exit(int status)`
  - Terminates with an *exit* status of `status`
  - Convention: normal return status is 0, nonzero on error
  - Another way to explicitly set the exit status is to return an integer value from the main routine

→ 현재 process로 돌아오지 않는다

- `exit` is called **once** but **never** returns.

Creating Processes

- *Parent process* creates a new running child process by calling `fork`

  fork()로 생긴 두 process 모두 비슷하지만 다른 memory를 사용하는 서로 다른 process

- `int fork(void)`

  fork() 호출 후 부모와 자식으로 나뉨 → return 값이 2가지

  자식 process로 리턴

  - Returns 0 to the child process, child's PID to parent process

    부모 process로 리턴

  - Child is ***almost*** identical to parent:
    - Child get an identical (but separate) copy of the parent's virtual address space
    - Child gets identical copies of the parent's open file descriptors
    - Child has a different PID than the parent

- `fork` is interesting (and often confusing) because it is called **once** but returns **twice**

fork Example

```
int main()
{
    pid_t pid;
    int x = 1;

    pid = Fork();
    if (pid == 0) {  /* Child */
        printf("child : x=%d\n", ++x);
       exit(0);
    }

    /* Parent */
    printf("parent: x=%d\n", --x);
    exit(0);
}
```

fork.c

```
linux> ./fork
parent: x=0
child : x=2
```

부모와 자식이 다른
memory에 x의 저장

- Call once, return twice
- Concurrent execution
  - Can't predict execution order of parent and child
- Duplicate but separate address space
  - `x` has a value of 1 when `fork()` returns in parent and child
  - Subsequenct changes to `x` are independent
- Shared open files
  - **`stdout`** is the same in both parent and child

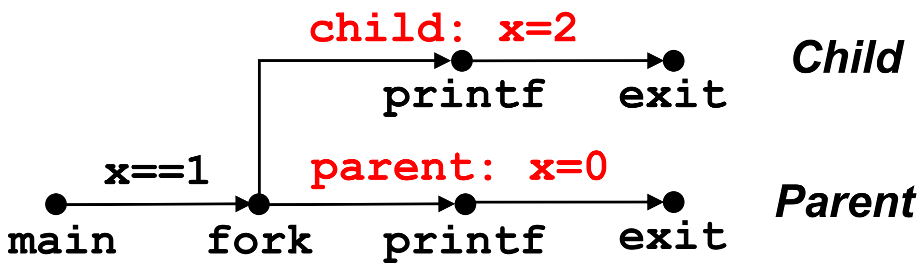
Modeling `fork` with Process Graphs

- A ***process graph*** is a useful tool for capturing the partial ordering of statements in a concurrent program:
  - Each vertex is the execution of a statement
  - `a` → `b` means `a` happens before `b`
  - Edges can be labeled with current value of variables
  - `printf` vertices can be labeled with output
  - Each graph begins with a vertex with no inedges
- Any ***topological sort*** of the graph corresponds to a feasible total ordering
  - Total ordering of vertices where all edges point from left to right

Process Graph Example

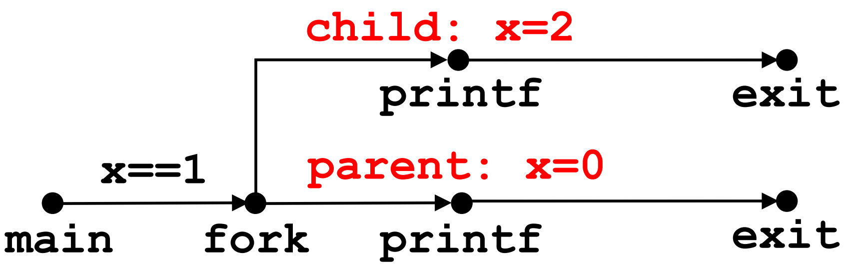
```c
int main()
{
    pid_t pid;
    int x = 1;

    pid = Fork();
    if (pid == 0) {  /* Child */
        printf("child : x=%d\n", ++x);
        exit(0);
    }

    /* Parent */
    printf("parent: x=%d\n", --x);
    exit(0);
}
```

fork.c

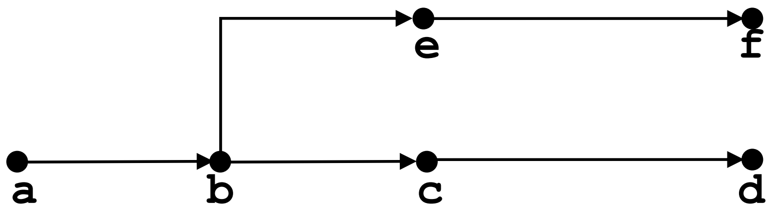


Interpreting Process Graphs

- Original graph:

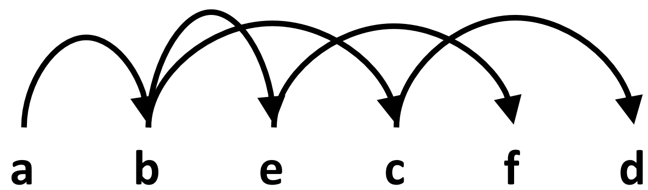


- Relabled graph:

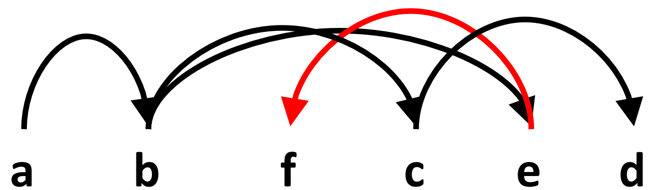


가능한

Feasible total ordering:



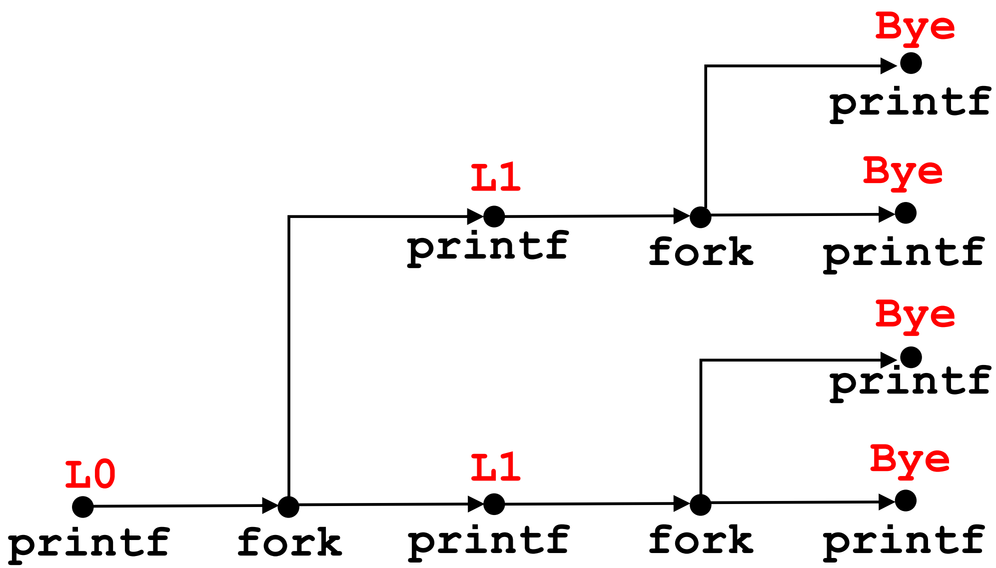
Infeasible total ordering:



f → e는 불가능

fork Example: Two consecutive forks

```
void fork2()
{
    printf("L0\n");
    fork();
    printf("L1\n");
    fork();
    printf("Bye\n");
}                         forks.c
```



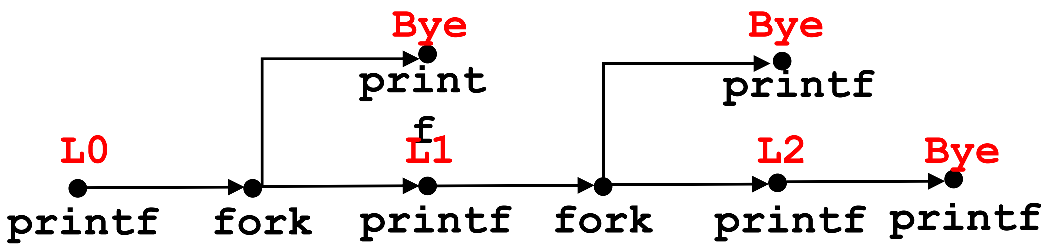
Feasible output:
L0
L1
Bye
Bye
L1
Bye
Bye

Infeasible output:
L0
Bye
L1
Bye
L1
Bye
Bye

fork Example: Nested forks in parent

```
void fork4()
{
    printf("L0\n");
    if (fork() != 0) {
        printf("L1\n");
        if (fork() != 0) {
            printf("L2\n");
        }
    }
    printf("Bye\n");
}
```

forks.c



Feasible output:

L0
L1
Bye
Bye
L2
Bye

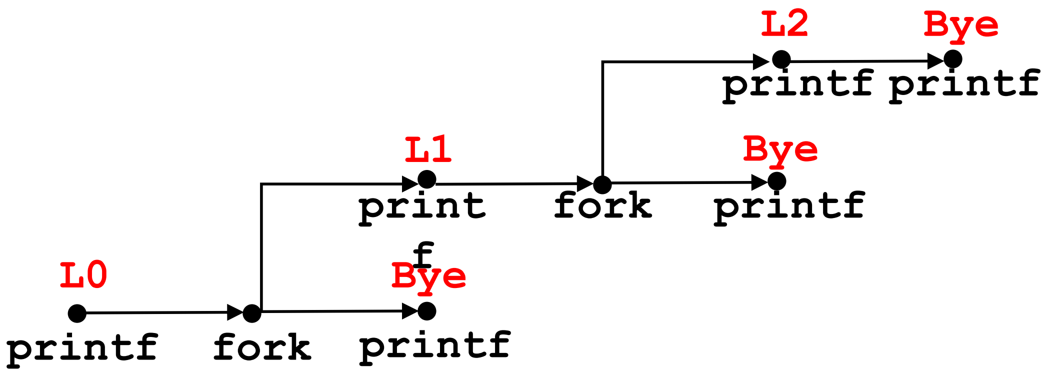
Infeasible output:

L0
Bye
L1
Bye
Bye
L2

fork Example: Nested forks in children

```
void fork5()
{
    printf("L0\n");
    if (fork() == 0) {
        printf("L1\n");
        if (fork() == 0) {
            printf("L2\n");
        }
    }
    printf("Bye\n");
}
```

forks.c



Feasible output:
L0
Bye
L1
L2
Bye
Bye

Infeasible output:
L0
Bye
L1
Bye
Bye
L2

Reaping Child Processes

- Idea
  - When process terminates, it still consumes system resources
    - Examples: Exit status, various OS tables
  - Called a "zombie" → process는 종료, 상태 정보 저장하기 위해서 메모리에 남아있는 process
    - Living corpse, half alive and half dead
- Reaping → process 정보를 제거 / 운영체제가 진행 (system call)
  - Performed by parent on terminated child (using `wait` or `waitpid`)
  - Parent is given exit status information
  - Kernel then deletes zombie child process
- What if parent doesn't reap?
  - If any parent terminates without reaping a child, then the orphaned child will be reaped by $\boxed{\texttt{init}\text{ process (pid == 1)}}$ → 모든 process의 부모 process
  - So, only need explicit reaping in long-running processes
    - e.g., shells and servers

Zombie Example

```c
void fork7() {
    if (fork() == 0) {
        /* Child */
        printf("Terminating Child, PID = %d\n", getpid());
        exit(0);
    } else {
        printf("Running Parent, PID = %d\n", getpid());
        while (1); /* Infinite loop */
    }    종X
}
```

forks.c

```
linux> ./forks 7 &
[1] 6639
Running Parent, PID = 6639
Terminating Child, PID = 6640
linux> ps
  PID TTY          TIME CMD
 6585 ttyp9    00:00:00 tcsh
 6639 ttyp9    00:00:03 forks
 6640 ttyp9    00:00:00 forks <defunct>
 6641 ttyp9    00:00:00 ps
linux> kill 6639
[1]    Terminated
linux> ps
  PID TTY          TIME CMD
 6585 ttyp9    00:00:00 tcsh
 6642 ttyp9    00:00:00 ps
```

`ps` shows child process as “defunct” (i.e., a zombie)

Killing parent allows child to be reaped by `init`

Non-terminating Child Example

자식 process의 정보를 받을 부모 process가 없음
↓
명시적으로 제거해야 한다.

```
void fork8() {
    if (fork() == 0) {
        /* Child */
        printf("Running Child, PID = %d\n",
               getpid());
        while (1); /* Infinite loop */
    } else {
        printf("Terminating Parent, PID = %d\n",
               getpid());
        exit(0);
    }
}
```

forks.c

```
linux> ./forks 8
Terminating Parent, PID = 6675
Running Child, PID = 6676
linux> ps
  PID TTY          TIME CMD
 6585 ttyp9    00:00:00 tcsh
 6676 ttyp9    00:00:06 forks
 6677 ttyp9    00:00:00 ps
linux> kill 6676
linux> ps
  PID TTY          TIME CMD
 6585 ttyp9    00:00:00 tcsh
 6678 ttyp9    00:00:00 ps
```

Child process still active even though parent has terminated

Must kill child explicitly, or else will keep running indefinitely

wait: Synchronizing with Children

System call

↳ 부모-자식 process 간의 실행순서를 정할 수 있다.

→ 부모가 자식을 reaping

→ 부모가 자식 process 종료시까지 기다리도록 한다

- Parent reaps a child by calling the `wait` function

자식 process → exit( )

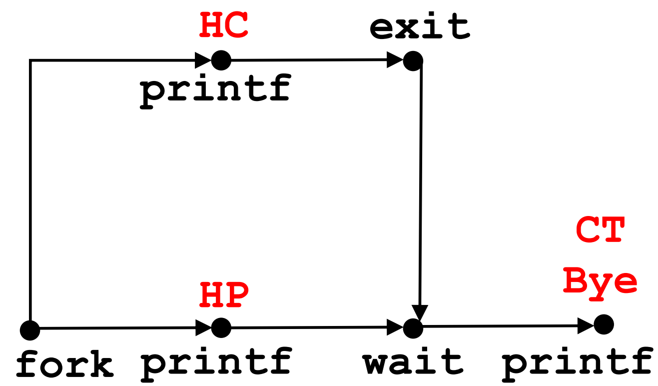
Pointer를 통하여 확인

- `int wait(int* child_status)`
  - Suspends current process until one of its children terminates
  - Return value is the **`pid`** of the child process that terminated
  - If **`child_status != NULL`**, then the integer it points to will be set to a value that indicates reason the child terminated and the exit status:
    - Checked using macros defined in `wait.h`
      - `WIFEXITED, WEXITSTATUS, WIFSIGNALED, WTERMSIG, WIFSTOPPED, WSTOPSIG, WIFCONTINUED`
      - See textbook for details

wait: Synchronizing with Children

```
void fork9() {
    int child_status;

    if (fork() == 0) {
        printf("HC: hello from child\n");
       exit(0);
    } else {
        printf("HP: hello from parent\n");
        wait(&child_status);
        printf("CT: child has terminated\n");
    }
    printf("Bye\n");
}
```

forks.c



(HC→CT)를 보장

Feasible output:
HC
HP
CT
Bye

Infeasible output:
HP
CT
Bye
HC

Another `wait` Example

- If multiple children completed, will take in arbitrary order
- Can use macros `WIFEXITED` and `WEXITSTATUS` to get information about exit status

```
void fork10() {
    pid_t pid[N];
    int i, child_status;
    for (i = 0; i < N; i++)
        if ((pid[i] = fork()) == 0) {
            exit(100+i); /* Child */
        }
    for (i = 0; i < N; i++) { /* Parent */
        pid_t wpid = wait(&child_status);
        if (WIFEXITED(child_status))
            printf("Child %d terminated with exit status %d\n",
                   wpid, WEXITSTATUS(child_status));
        else
            printf("Child %d terminate abnormally\n", wpid);
    }
}
```

forks.c

waitpid: Waiting for a Specific Process

pid에 해당하는 process가 끝난후에는 Return

- pid_t waitpid(pid_t pid, int* status, int options)
  - Suspends current process until specific process terminates
  - Various options (see textbook)

```
void fork11() {
    pid_t pid[N];
    int i;
    int child_status;

    for (i = 0; i < N; i++)
        if ((pid[i] = fork()) == 0)
            exit(100+i); /* Child */
    for (i = N-1; i >= 0; i--) {
        pid_t wpid = waitpid(pid[i], &child_status, 0);
        if (WIFEXITED(child_status))
            printf("Child %d terminated with exit status %d\n",
                   wpid, WEXITSTATUS(child_status));
        else
            printf("Child %d terminate abnormally\n", wpid);
    }
}
```

forks.c

execve: Loading and Running Programs

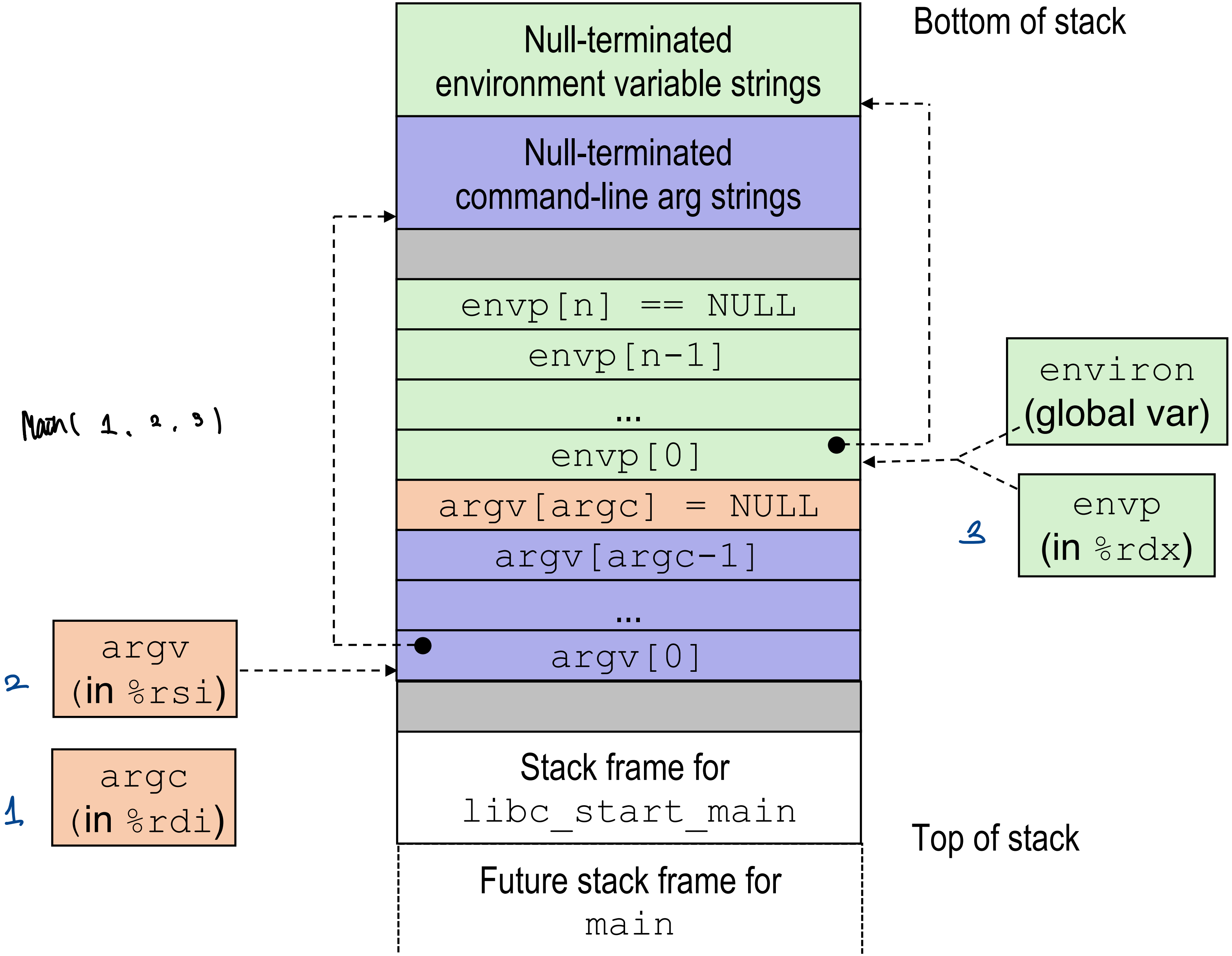
- `int execve(char *filename, char *argv[], char *envp[])`

  실행파일의 위치

- Loads and runs in the current process:
  - Executable file **`filename`**
    - Can be object file or script file beginning with `#!interpreter` (e.g., `#!/bin/bash`)
  - …with argument list **`argv`**
    - By convention **`argv[0]==filename`**
  - …and environment variable list **`envp`**
    - "name=value" strings (e.g., `USER=droh`)
    - `getenv, putenv, printenv`
- Overwrites code, data, and stack
  - Retains PID, open files and signal context
- Called once and never returns
  - …except if there is an error

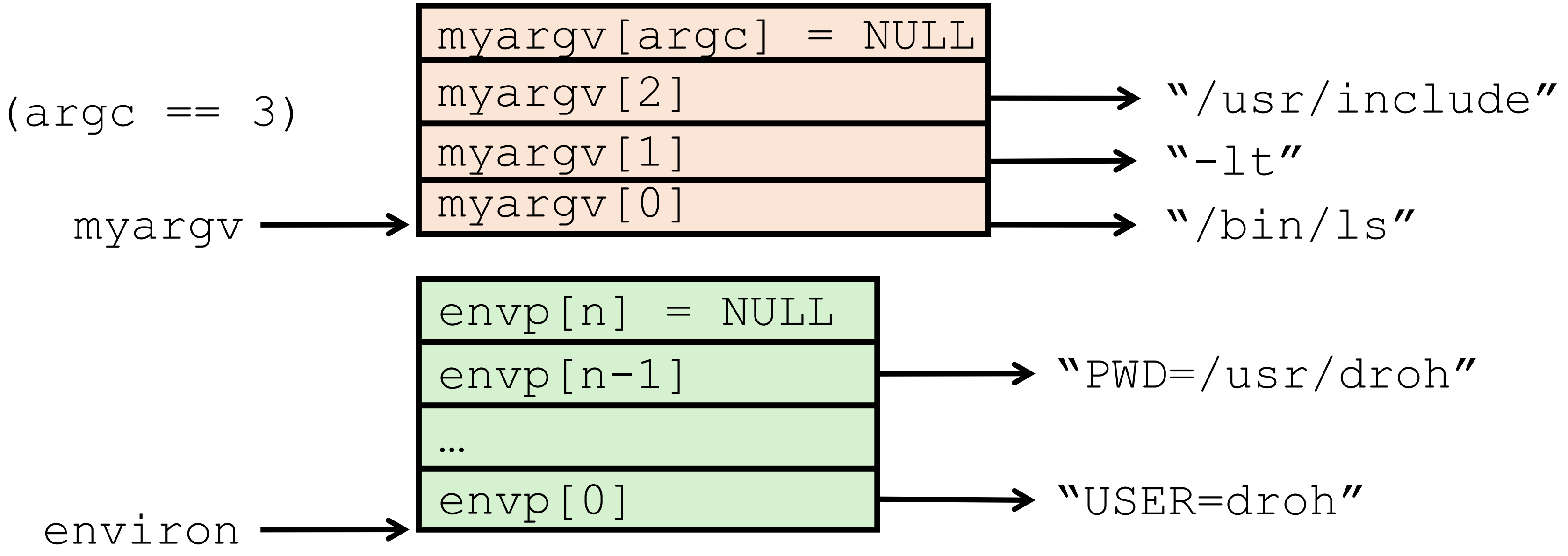
execve (≠fork)
→ 자식 process를 부모 process와 같은 프로그램이 아닌 다른 소스코드를 가지도록 하는 명령어

Structure of Stack When a Program Starts



execve Example

- Executes `/bin/ls -lt /usr/include` in child process using current environment




```c
if ((pid = Fork()) == 0) {   /* Child runs program */
    if (execve(myargv[0], myargv, environ) < 0) {
        printf("%s: Command not found.\n", myargv[0]);
        exit(1);
    }
}
```

Summary

- Exceptions
  - Events that require nonstandard control flow
  - Generated externally (interrupts) or internally (traps and faults)

- Processes
  - At any given time, system has multiple active processes
  - Only one can execute at a time on a single core, though
  - Each process appears to have total control of processor + private memory space

Summary (cont.)

- Spawning processes
  - Call `fork`
  - One call, two returns
- Process completion
  - Call `exit`
  - One call, no return
- Reaping and waiting for processes
  - Call `wait` or `waitpid`
- Loading and running programs
  - Call `execve` (or variant)
  - One call, (normally) no return