4

The Abstraction: The Process

In this chapter, we discuss one of the most fundamental abstractions that the OS provides to users: the **process**. The definition of a process, infor mally, is quite simple: it is a **running program** [V+65,BH70]. The program itself is a lifeless thing: it just sits there on the disk, a bunch of instructions (and maybe some static data), waiting to spring into action. It is the oper ating system that takes these bytes and gets them running, transforming the program into something useful.

It turns out that one often wants to run more than one program at once; for example, consider your desktop or laptop where you might like to run a web browser, mail program, a game, a music player, and so forth. In fact, a typical system may be seemingly running tens or even hundreds of processes at the same time. Doing so makes the system easy to use, as one never need be concerned with whether a CPU is available; one simply runs programs. Hence our challenge:

THE CRUX OF THE PROBLEM:

HOW TO PROVIDE THE ILLUSION OF MANY CPUS?

Although there are only a few physical CPUs available, how can the OS provide the illusion of a nearly-endless supply of said CPUs?

The OS creates this illusion by **virtualizing** the CPU. By running one process, then stopping it and running another, and so forth, the OS can promote the illusion that many virtual CPUs exist when in fact there is only one physical CPU (or a few). This basic technique, known as **time sharing** of the CPU, allows users to run as many concurrent processes as they would like; the potential cost is performance, as each will run more slowly if the CPU(s) must be shared.

To implement virtualization of the CPU, and to implement it well, the OS will need both some low-level machinery and some high-level in telligence. We call the low-level machinery **mechanisms**; mechanisms are low-level methods or protocols that implement a needed piece of functionality. For example, we’ll learn later how to implement a **context**

1

2 THE ABSTRACTION: THE PROCESS

TIP: USE TIME SHARING (AND SPACE SHARING)

**Time sharing** is a basic technique used by an OS to share a resource. By allowing the resource to be used for a little while by one entity, and then a little while by another, and so forth, the resource in question (e.g., the CPU, or a network link) can be shared by many. The counterpart of time sharing is **space sharing**, where a resource is divided (in space) among those who wish to use it. For example, disk space is naturally a space shared resource; once a block is assigned to a file, it is normally not as signed to another file until the user deletes the original file.

**switch**, which gives the OS the ability to stop running one program and start running another on a given CPU; this **time-sharing** mechanism is employed by all modern OSes.

On top of these mechanisms resides some of the intelligence in the OS, in the form of **policies**. Policies are algorithms for making some kind of decision within the OS. For example, given a number of possi ble programs to run on a CPU, which program should the OS run? A **scheduling policy** in the OS will make this decision, likely using histori cal information (e.g., which program has run more over the last minute?), workload knowledge (e.g., what types of programs are run), and perfor mance metrics (e.g., is the system optimizing for interactive performance, or throughput?) to make its decision.

4.1 The Abstraction: A Process

The abstraction provided by the OS of a running program is something we will call a **process**. As we said above, a process is simply a running program; at any instant in time, we can summarize a process by taking an inventory of the different pieces of the system it accesses or affects during the course of its execution.

To understand what constitutes a process, we thus have to understand its **machine state**: what a program can read or update when it is running. At any given time, what parts of the machine are important to the execu tion of this program?

One obvious component of machine state that comprises a process is its memory. Instructions lie in memory; the data that the running pro gram reads and writes sits in memory as well. Thus the memory that the process can address (called its **address space**) is part of the process.

Also part of the process’s machine state are registers; many instructions explicitly read or update registers and thus clearly they are important to the execution of the process.

Note that there are some particularly special registers that form part of this machine state. For example, the **program counter** (**PC**) (sometimes called the **instruction pointer** or **IP**) tells us which instruction of the pro gram will execute next; similarly a **stack pointer** and associated **frame**

OPERATING

SYSTEMS

[VERSION 1.01]

WWW.OSTEP.ORG

THE ABSTRACTION: THE PROCESS 3

TIP: SEPARATE POLICY AND MECHANISM

In many operating systems, a common design paradigm is to separate high-level policies from their low-level mechanisms [L+75]. You can think of the mechanism as providing the answer to a how question about a system; for example, how does an operating system perform a context switch? The policy provides the answer to a which question; for example, which process should the operating system run right now? Separating the two allows one easily to change policies without having to rethink the mechanism and is thus a form of **modularity**, a general software design principle.

**pointer** are used to manage the stack for function parameters, local vari ables, and return addresses.

Finally, programs often access persistent storage devices too. Such I/O

information might include a list of the files the process currently has open.

4.2 Process API

Though we defer discussion of a real process API until a subsequent

chapter, here we first give some idea of what must be included in any interface of an operating system. These APIs, in some form, are available on any modern operating system.

• **Create:** An operating system must include some method to cre

ate new processes. When you type a command into the shell, or

double-click on an application icon, the OS is invoked to create a

new process to run the program you have indicated.

• **Destroy:** As there is an interface for process creation, systems also

provide an interface to destroy processes forcefully. Of course, many

processes will run and just exit by themselves when complete; when

they don’t, however, the user may wish to kill them, and thus an in

terface to halt a runaway process is quite useful.

• **Wait:** Sometimes it is useful to wait for a process to stop running;

thus some kind of waiting interface is often provided.

• **Miscellaneous Control:** Other than killing or waiting for a process,

there are sometimes other controls that are possible. For example,

most operating systems provide some kind of method to suspend a

process (stop it from running for a while) and then resume it (con

tinue it running).

• **Status:** There are usually interfaces to get some status information

about a process as well, such as how long it has run for, or what

state it is in.

c 2008–19, ARPACI-DUSSEAUTHREE

EASY PIECES

4 THE ABSTRACTION: THE PROCESS

CPU Memory

code

static data

heap

stack

Process

code

static data

Program Loading:

Takes on-disk program

and reads it into the

address space of process

Disk

Figure 4.1: **Loading: From Program To Process**

4.3 Process Creation: A Little More Detail

One mystery that we should unmask a bit is how programs are trans formed into processes. Specifically, how does the OS get a program up and running? How does process creation actually work?

The first thing that the OS must do to run a program is to **load** its code and any static data (e.g., initialized variables) into memory, into the ad dress space of the process. Programs initially reside on **disk** (or, in some modern systems, **flash-based SSDs**) in some kind of **executable format**; thus, the process of loading a program and static data into memory re quires the OS to read those bytes from disk and place them in memory somewhere (as shown in Figure 4.1).

In early (or simple) operating systems, the loading process is done **ea gerly**, i.e., all at once before running the program; modern OSes perform the process **lazily**, i.e., by loading pieces of code or data only as they are needed during program execution. To truly understand how lazy loading of pieces of code and data works, you’ll have to understand more about

OPERATING

SYSTEMS

[VERSION 1.01]

WWW.OSTEP.ORG

THE ABSTRACTION: THE PROCESS 5

the machinery of **paging** and **swapping**, topics we’ll cover in the future when we discuss the virtualization of memory. For now, just remember that before running anything, the OS clearly must do some work to get the important program bits from disk into memory.

Once the code and static data are loaded into memory, there are a few

other things the OS needs to do before running the process. Some mem ory must be allocated for the program’s **run-time stack** (or just **stack**). As you should likely already know, C programs use the stack for local variables, function parameters, and return addresses; the OS allocates this memory and gives it to the process. The OS will also likely initial ize the stack with arguments; specifically, it will fill in the parameters to the main() function, i.e., argc and the argv array.

The OS may also allocate some memory for the program’s **heap**. In C

programs, the heap is used for explicitly requested dynamically-allocated data; programs request such space by calling malloc() and free it ex plicitly by calling free(). The heap is needed for data structures such as linked lists, hash tables, trees, and other interesting data structures. The heap will be small at first; as the program runs, and requests more mem ory via the malloc() library API, the OS may get involved and allocate more memory to the process to help satisfy such calls.

The OS will also do some other initialization tasks, particularly as re

lated to input/output (I/O). For example, in UNIX systems, each process by default has three open **file descriptors**, for standard input, output, and error; these descriptors let programs easily read input from the terminal and print output to the screen. We’ll learn more about I/O, file descrip tors, and the like in the third part of the book on **persistence**.

By loading the code and static data into memory, by creating and ini

tializing a stack, and by doing other work as related to I/O setup, the OS has now (finally) set the stage for program execution. It thus has one last task: to start the program running at the entry point, namely main(). By jumping to the main() routine (through a specialized mechanism that we will discuss next chapter), the OS transfers control of the CPU to the newly-created process, and thus the program begins its execution.

4.4 Process States

Now that we have some idea of what a process is (though we will

continue to refine this notion), and (roughly) how it is created, let us talk about the different **states** a process can be in at a given time. The notion that a process can be in one of these states arose in early computer systems [DV66,V+65]. In a simplified view, a process can be in one of three states:

• **Running**: In the running state, a process is running on a processor.

This means it is executing instructions.

• **Ready**: In the ready state, a process is ready to run but for some

reason the OS has chosen not to run it at this given moment.

c 2008–19, ARPACI-DUSSEAUTHREE

EASY PIECES

6 THE ABSTRACTION: THE PROCESS

Descheduled

Running Ready

Scheduled

I/O: initiate I/O: done

Blocked

Figure 4.2: **Process: State Transitions**

• **Blocked**: In the blocked state, a process has performed some kind of operation that makes it not ready to run until some other event takes place. A common example: when a process initiates an I/O request to a disk, it becomes blocked and thus some other process can use the processor.

If we were to map these states to a graph, we would arrive at the di agram in Figure 4.2. As you can see in the diagram, a process can be moved between the ready and running states at the discretion of the OS. Being moved from ready to running means the process has been **sched uled**; being moved from running to ready means the process has been **descheduled**. Once a process has become blocked (e.g., by initiating an I/O operation), the OS will keep it as such until some event occurs (e.g., I/O completion); at that point, the process moves to the ready state again (and potentially immediately to running again, if the OS so decides).

Let’s look at an example of how two processes might transition through some of these states. First, imagine two processes running, each of which only use the CPU (they do no I/O). In this case, a trace of the state of each process might look like this (Figure 4.3).

**Time Process**0 **Process**1 **Notes**

1 Running Ready

2 Running Ready

3 Running Ready

4 Running Ready Process0 now done

5 – Running

6 – Running

7 – Running

8 – Running Process1 now done

Figure 4.3: **Tracing Process State: CPU Only**

OPERATING

SYSTEMS

[VERSION 1.01]

WWW.OSTEP.ORG

THE ABSTRACTION: THE PROCESS 7

**Time Process**0 **Process**1 **Notes**

1 Running Ready

2 Running Ready

3 Running Ready Process0 initiates I/O

4 Blocked Running Process0 is blocked,

5 Blocked Running so Process1 runs

6 Blocked Running

7 Ready Running I/O done

8 Ready Running Process1 now done

9 Running –

10 Running – Process0 now done

Figure 4.4: **Tracing Process State: CPU and I/O**

In this next example, the first process issues an I/O after running for

some time. At that point, the process is blocked, giving the other process a chance to run. Figure 4.4 shows a trace of this scenario.

More specifically, Process0 initiates an I/O and becomes blocked wait ing for it to complete; processes become blocked, for example, when read ing from a disk or waiting for a packet from a network. The OS recog nizes Process0 is not using the CPU and starts running Process1. While Process1 is running, the I/O completes, moving Process0 back to ready. Finally, Process1 finishes, and Process0 runs and then is done.

Note that there are many decisions the OS must make, even in this

simple example. First, the system had to decide to run Process1 while Process0 issued an I/O; doing so improves resource utilization by keep ing the CPU busy. Second, the system decided not to switch back to Process0 when its I/O completed; it is not clear if this is a good deci sion or not. What do you think? These types of decisions are made by the OS **scheduler**, a topic we will discuss a few chapters in the future.

4.5 Data Structures

The OS is a program, and like any program, it has some key data struc

tures that track various relevant pieces of information. To track the state of each process, for example, the OS likely will keep some kind of **pro cess list** for all processes that are ready and some additional informa tion to track which process is currently running. The OS must also track, in some way, blocked processes; when an I/O event completes, the OS should make sure to wake the correct process and ready it to run again.

Figure 4.5 shows what type of information an OS needs to track about

each process in the xv6 kernel [CK+08]. Similar process structures exist in “real” operating systems such as Linux, Mac OS X, or Windows; look them up and see how much more complex they are.

From the figure, you can see a couple of important pieces of informa

tion the OS tracks about a process. The **register context** will hold, for a c 2008–19, ARPACI-DUSSEAUTHREE

EASY PIECES

8 THE ABSTRACTION: THE PROCESS

// the registers xv6 will save and restore

// to stop and subsequently restart a process

struct context {

int eip;

int esp;

int ebx;

int ecx;

int edx;

int esi;

int edi;

int ebp;

};

// the different states a process can be in

enum proc\_state { UNUSED, EMBRYO, SLEEPING,

RUNNABLE, RUNNING, ZOMBIE };

// the information xv6 tracks about each process

// including its register context and state

struct proc {

char \*mem; // Start of process memory uint sz; // Size of process memory char \*kstack; // Bottom of kernel stack // for this process

enum proc\_state state; // Process state

int pid; // Process ID

struct proc \*parent; // Parent process

void \*chan; // If !zero, sleeping on chan int killed; // If !zero, has been killed struct file \*ofile[NOFILE]; // Open files

struct inode \*cwd; // Current directory

struct context context; // Switch here to run process struct trapframe \*tf; // Trap frame for the

// current interrupt

};

Figure 4.5: **The xv6 Proc Structure**

stopped process, the contents of its registers. When a process is stopped, its registers will be saved to this memory location; by restoring these reg isters (i.e., placing their values back into the actual physical registers), the OS can resume running the process. We’ll learn more about this technique known as a **context switch** in future chapters.

You can also see from the figure that there are some other states a pro

cess can be in, beyond running, ready, and blocked. Sometimes a system will have an **initial** state that the process is in when it is being created. Also, a process could be placed in a **final** state where it has exited but

OPERATING

SYSTEMS

[VERSION 1.01]

WWW.OSTEP.ORG

THE ABSTRACTION: THE PROCESS 9

ASIDE: DATA STRUCTURE — THE PROCESS LIST

Operating systems are replete with various important **data structures** that we will discuss in these notes. The **process list** (also called the **task list**) is the first such structure. It is one of the simpler ones, but certainly any OS that has the ability to run multiple programs at once will have something akin to this structure in order to keep track of all the running programs in the system. Sometimes people refer to the individual struc ture that stores information about a process as a **Process Control Block** (**PCB**), a fancy way of talking about a C structure that contains informa tion about each process (also sometimes called a **process descriptor**).

has not yet been cleaned up (in UNIX-based systems, this is called the **zombie** state1). This final state can be useful as it allows other processes (usually the **parent** that created the process) to examine the return code of the process and see if the just-finished process executed successfully (usually, programs return zero in UNIX-based systems when they have accomplished a task successfully, and non-zero otherwise). When fin ished, the parent will make one final call (e.g., wait()) to wait for the completion of the child, and to also indicate to the OS that it can clean up any relevant data structures that referred to the now-extinct process.

4.6 Summary

We have introduced the most basic abstraction of the OS: the process.

It is quite simply viewed as a running program. With this conceptual view in mind, we will now move on to the nitty-gritty: the low-level mechanisms needed to implement processes, and the higher-level poli cies required to schedule them in an intelligent way. By combining mech anisms and policies, we will build up our understanding of how an oper ating system virtualizes the CPU.

1Yes, the zombie state. Just like real zombies, these zombies are relatively easy to kill.

However, different techniques are usually recommended.

c 2008–19, ARPACI-DUSSEAUTHREE

EASY PIECES

10 THE ABSTRACTION: THE PROCESS

ASIDE: KEY PROCESS TERMS

• The **process** is the major OS abstraction of a running program. At any point in time, the process can be described by its state: the con tents of memory in its **address space**, the contents of CPU registers (including the **program counter** and **stack pointer**, among others), and information about I/O (such as open files which can be read or written).

• The **process API** consists of calls programs can make related to pro cesses. Typically, this includes creation, destruction, and other use ful calls.

• Processes exist in one of many different **process states**, including running, ready to run, and blocked. Different events (e.g., getting scheduled or descheduled, or waiting for an I/O to complete) tran sition a process from one of these states to the other.

• A **process list** contains information about all processes in the sys tem. Each entry is found in what is sometimes called a **process control block** (**PCB**), which is really just a structure that contains information about a specific process.

OPERATING

SYSTEMS

[VERSION 1.01]

WWW.OSTEP.ORG

THE ABSTRACTION: THE PROCESS 11

**References**

[BH70] “The Nucleus of a Multiprogramming System” by Per Brinch Hansen. Communica tions of the ACM, Volume 13:4, April 1970. This paper introduces one of the first **microkernels** in operating systems history, called Nucleus. The idea of smaller, more minimal systems is a theme that rears its head repeatedly in OS history; it all began with Brinch Hansen’s work described herein.

[CK+08] “The xv6 Operating System” by Russ Cox, Frans Kaashoek, Robert Morris, Nickolai Zeldovich. From: https://github.com/mit-pdos/xv6-public. The coolest real and little OS in the world. Download and play with it to learn more about the details of how operating systems actually work. We have been using an older version (2012-01-30-1-g1c41342) and hence some examples in the book may not match the latest in the source.

[DV66] “Programming Semantics for Multiprogrammed Computations” by Jack B. Dennis, Earl C. Van Horn. Communications of the ACM, Volume 9, Number 3, March 1966 . This paper defined many of the early terms and concepts around building multiprogrammed systems.

[L+75] “Policy/mechanism separation in Hydra” by R. Levin, E. Cohen, W. Corwin, F. Pollack, W. Wulf. SOSP ’75, Austin, Texas, November 1975. An early paper about how to structure operat ing systems in a research OS known as Hydra. While Hydra never became a mainstream OS, some of its ideas influenced OS designers.

[V+65] “Structure of the Multics Supervisor” by V.A. Vyssotsky, F. J. Corbato, R. M. Graham. Fall Joint Computer Conference, 1965. An early paper on Multics, which described many of the basic ideas and terms that we find in modern systems. Some of the vision behind computing as a utility are finally being realized in modern cloud systems.

c 2008–19, ARPACI-DUSSEAUTHREE

EASY PIECES

12 THE ABSTRACTION: THE PROCESS

**Homework (Simulation)**

This program, process-run.py, allows you to see how process states change as programs run and either use the CPU (e.g., perform an add instruction) or do I/O (e.g., send a request to a disk and wait for it to complete). See the README for details.

**Questions**

1. Run process-run.py with the following flags: -l 5:100,5:100. What should the CPU utilization be (e.g., the percent of time the

CPU is in use?) Why do you know this? Use the -c and -p flags to

see if you were right.

2. Now run with these flags: ./process-run.py -l 4:100,1:0. These flags specify one process with 4 instructions (all to use the

CPU), and one that simply issues an I/O and waits for it to be done.

How long does it take to complete both processes? Use -c and -p

to find out if you were right.

3. Switch the order of the processes: -l 1:0,4:100. What happens now? Does switching the order matter? Why? (As always, use -c

and -p to see if you were right)

4. We’ll now explore some of the other flags. One important flag is -S, which determines how the system reacts when a process is

sues an I/O. With the flag set to SWITCH ON END, the system

will NOT switch to another process while one is doing I/O, in

stead waiting until the process is completely finished. What hap

pens when you run the following two processes (-l 1:0,4:100

-c -S SWITCH ON END), one doing I/O and the other doing CPU

work?

5. Now, run the same processes, but with the switching behavior set to switch to another process whenever one is WAITING for I/O (-l

1:0,4:100 -c -S SWITCH ON IO). What happens now? Use -c

and -p to confirm that you are right.

6. One other important behavior is what to do when an I/O com pletes. With -I IO RUN LATER, when an I/O completes, the pro

cess that issued it is not necessarily run right away; rather, whatever

was running at the time keeps running. What happens when you

run this combination of processes? (Run ./process-run.py -l

3:0,5:100,5:100,5:100 -S SWITCH ON IO -I IO RUN LATER -c -p) Are system resources being effectively utilized?

7. Now run the same processes, but with -I IO RUN IMMEDIATE set, which immediately runs the process that issued the I/O. How does

this behavior differ? Why might running a process that just com

pleted an I/O again be a good idea?

OPERATING

SYSTEMS

[VERSION 1.01]

WWW.OSTEP.ORG

THE ABSTRACTION: THE PROCESS 13

8. Now run with some randomly generated processes: -s 1 -l 3:50,3:50 or -s 2 -l 3:50,3:50 or -s 3 -l 3:50,3:50. See if you can predict how the trace will turn out. What happens when you use the flag -I IO RUN IMMEDIATE vs. -I IO RUN LATER? What hap pens when you use -S SWITCH ON IO vs. -S SWITCH ON END?

c 2008–19, ARPACI-DUSSEAUTHREE

EASY PIECES