System View of a Process

The process manager implements the process abstraction. It covers the following areas:

- Scheduling of processes on the CPU(s)
- Synchronization mechanisms for processes
- Responsible for dealing with deadlocks among processes
- Partially responsible for protection and security
Process Manager Overview
A program is a set of source code modules that reference each other and reference a collection of library object modules.

The *address space* is a set of linearly ordered locations used by the process to reference program text, data, operating system services, resources etc.

A program *image* defines the set of all primary memory addresses a process uses.
Generating the Address Space

- Compiling and linking produces an absolute program (a.out).
- The loader maps the address space to the allocated primary memory addresses and sets the PC (program counter) to the first executable instruction (a.k.a. main entry point).
The Structure of Executable Files

- The structure of an executable file is dependent upon the operating system.
- The compiler/linker needs to produce a file in one the formats understood by the operating system to be executable.
- Older standard executable formats from Unix: **COFF** (Common Object File Format) and **a.out**
  - Linux and most modern Unixes use the **ELF** (Executable and Linkable Format) format.
  - MS Windows uses the **PE** (Portable Executable, derived from the COFF format) format.
  - MAC OS X uses the **Mach-O** format (derived from the a.out format).
The ELF Executable format

- Flexible and extensible, not bound to any particular processor or architecture
- Each ELF file is made up of one ELF header that describes the layout of the files. Then physical (or program) headers describe the program segments. These include the text segment, read only data and data segments. Section header table describes information useful for linking and loading
- The actual compiled code or text, the actual read only data and data segment that contained initialized global and static variables
- The executable image on the disk does not have space for uninitialized data. The uninitialized data is set to zero after being loaded into memory. This saves disk space and makes program start-up faster
- The whole executable text is not loaded, rather page faults are allowed to bring in the executable as needed (demand loading)
- ELF uses position independent code and a global offset table, which trades off execution time against memory usage in favor of the latter
<table>
<thead>
<tr>
<th>Code</th>
<th>Data</th>
</tr>
</thead>
</table>
| 'E' 'L' 'F'         | ELF Executable Image (statically linked file)  
| 0x8048090           |  
| 52                  |  
| 32                  |  
| 2                   |  
| ...                 |  
| PT_LOAD             |  
| 0                   |  
| 0x8048000           |  
| 68532               |  
| 68532               |  
| PF_R, PF_X          |  
| PT_LOAD             |  
| 68536               |  
| 0x8059BB8           |  
| 2200                |  
| 4248                |  
| PF_R, PF_W          |  

The table illustrates the ELF file format, showing various fields such as types, offsets, and addresses.
ELF layout

- How to look at executables: one way is to use the dump command `od` It has various options to examine the data in hex, octal, ASCII etc. Under KDE there is a utility called `okteta` that is a nice GUI hex editor.
- Use the utility `readelf` to peek into the structure of an ELF file.
- Look at the header file `/usr/include/linux/elf.h` for more details of the ELF executable format.
- See example `process-management/display-elf-headers.c` for a program that reads headers from an ELF executable file.
- Dynamically linked executables have more segments due to linking with libraries.
Microsoft’s Portable Executable (PE) Format

- Based on the COFF (Common Object File Format from Unix). Retains the old MZ header from MS-DOS to remain backwards compatible. Works on all Windows operating systems since NT 3.1
- Consists of an MS-DOS MZ header, followed by a real-mode stub program, the PE file signature, the PE file header, the PE optional header, all of the section headers, and finally, all of the section bodies
- The PE file format has eleven predefined sections, as is common to applications for Windows API, but each application can define its own unique sections for code and data
- The `.debug` predefined section also has the capability of being stripped from the file into a separate debug file. If so, a special debug header is used to parse the debug file, and a flag is specified in the PE file header to indicate that the debug data has been stripped
Microsoft’s Portable Executable Format Layout

Microsoft’s Portable Executable (PE) Format

- The .NET framework uses an extended PE file format. There is another extension known as PE32+ (or PE+) for 64-bit systems as well as one for the embedded Windows CE system.
- PE files use a preferred base address and all addresses generated by the compiler/linker are fixed ahead of time to speed up execution. However, if the preferred base address isn’t available, then an expensive “rebasing” operation must be done that can result in having to copy shared libraries and causing a loss of memory efficiency.
- Under Linux/Unix, MS Windows binaries (PE format) can be executed under the wine environment http://www.winehq.org/.
Consistency in the Address Space

- **Memory Hierarchy:**
  Registers ← Primary Memory ← Secondary Memory.
  Registers ← on-chip Cache ← off-chip Cache ← Primary Memory ← Secondary Memory

- The memory hierarchy is consistent for locations that contain instructions (since programs are not allowed to be self-modifying). But the data values are not consistent unless the programmer explicitly makes them consistent

- For a given variable, we have its value in a register ($M_{R_i}$), its value in the primary memory ($M_{p_j}$), and its value in secondary memory ($M_{s_k}$)

- What happens when a CPU is switched to another process?
  What happens when memory manager deallocates some of the space used by a process?

- Linux system calls to synchronize memory images with disk images:
  - `fdatasync` - synchronize a file’s in-core data with that on disk
  - `sync` - synchronize a file’s complete in-core state with that on disk
The Process Descriptor

The process descriptor is the primary data structure used to keep track of the status of a process and the specific environment that is associated with a process. It contains the following types of information:

- process state (whether it is blocked or ready)
- memory state
- current processor register contents
- pointer to the stack for the process
- resources (those allocated and those waiting for)
- other information
A process descriptor is allocated when a process is created and deallocated when a process dies. Usually there is a limit on the number of process descriptors in an operating system.

Even though the process manager is the one primarily interacting with the process descriptor it is also queried and some fields are modified by other parts of the operating system.

How to find the process descriptor in Linux source code?
Start with the source code for `fork()` system call (in the file `kernel/fork.c`). The obvious candidate is the structure `task_struct`, which is found in the header file `include/linux/sched.h` in the kernel source. (Use `grep "task_struct {"` `*.h` in the directory `include/linux` in the kernel source code)
In Linux terminology, they are called *tasks*. Linux has a list of process descriptors (which are of type `task_struct` defined in `sched.h` in your Linux kernel source tree)

- The maximum number of threads/processes allowed is dependent upon the amount of memory in the system. Check `/proc/sys/kernel/threads-max` for the current limit.
- By writing to that file, the limit can be changed on the fly (by the superuser). Or set it in `/etc/sysctl.conf` to set it at bootup time.
- There is also a limit on max pid to be 32768 ($2^{15}$) to make 2.6 and newer kernels compatible with programs written for the older kernels. This limit can be seen in `/proc/sys/kernel/pid_max`
- This can be overwritten to any value up to $2^{22}$ (about 4 million). For example:
  ```bash
  echo 1000000 > /proc/sys/kernel/pid_max
  ```
  To do it permanently, add `kernel.pid_max = 1000000` to the `/etc/sysctl.conf` file so it gets set at bootup time.
- Look at `include/linux/threads.h` in kernel source code to see the limits.
Linux Process Descriptor

Browse live in the file `include/linux/sched.h` in the kernel source...some snippets given below.

```c
struct task_struct {
    volatile long state; /* -1 unrunnable, 0 runnable, >0 stopped */
    void *stack;
    atomic_t usage;
    unsigned int flags; /* per process flags, defined below */
    unsigned int ptrace;
    ...
    int prio, static_prio, normal_prio;
    unsigned int rt_priority;
    const struct sched_class *sched_class;
    struct sched_entity se;
    struct sched_rt_entity rt;
    ...
    struct mm_struct *mm, *active_mm;
    int exit_state;
    int exit_code, exit_signal;
    int pdeath_signal; /* The signal sent when the parent dies */
    ...
    pid_t pid;
    pid_t tgid;
```
/* pointers to (original) parent process, youngest child, younger sibling, *
 * older sibling, respectively. (p->father can be replaced with p->real_parent->pid) *
 */
struct task_struct *real_parent; /* real parent process */
struct task_struct *parent; /* recipient of SIGCHLD, wait4() reports */
/* children/sibling forms the list of my natural children */
struct list_head children; /* list of my children */
struct list_head sibling; /* linkage in my parent’s children list */
struct task_struct *group_leader; /* threadgroup leader */
...
/* PID/PID hash table linkage. */
struct pid_link pids[PIDTYPE_MAX];
struct list_head thread_group;
...
cputime_t utime, stime, utimescaled, stimescaled;
cputime_t gtime;
...
/* CPU-specific state of this task */
struct thread_struct thread;
/* filesystem information */
struct fs_struct *fs;
/* open file information */
struct files_struct *files;
/* signal handlers */
struct signal_struct *signal;
struct sighand_struct *sighand;
sigset_t blocked, real_blocked;
sigset_t saved_sigmask; /* restored if set_restore_sigmask() was used */
struct sigpending pending;
...
Data Structures for Processes

What data structure(s) are used to keep track of the processes?

- Linux kernel: The process descriptors are kept in circular linked lists, a binarization of a general tree data structure and a hash table simultaneously!

- The linked list implementation in the kernel uses the following node (check include/linux/types.h and include/linux/list.h):

  ```c
  struct list_head {
      struct list_head *next, *prev;
  };
  ```

- The linked lists are circular, so there is no head or tail node. We can traverse the whole list starting from any node.
The Linux Bootup Process

Systemd has replaced init process that was used traditionally in Linux/Unix systems.

The systems is a tree of processes with `init` or `systemd` the ancestor of all processes.
The `pstree` command on a machine running Linux shows the tree of processes.

```
kohinoor:pstree
init+-+crond
  |-2*[gvim]
  |-inetd
  |-kerneld
  |-kflushd
  |-klogd
  |-kswapd
  |-login---bash---startx---xinit+-+X
  |                   `-fvwm+-GoodStuff
  |                     `-ical
  |                      `-nxterm---bash+-netscape---netscaped
  |                           `-pstree
  |                      `-xbiff
  |                         `-xclock
  `-lpd
  `-5*[mingetty]
  `-4*[nfsiod]
  `-nxterm---bash
  `-portmap
  `-rpc.mountd
  `-rpc.nfsd
  `-rsh---rsh
  `-sendmail
  `-syslogd
  `-'update
```
MS Windows Processes

- Processes and Threads are kept track of in separate data structures.
- Each windows process is represented by a *executive process block*. It contains pointers to other structures, including *executive thread blocks*. Part of the information is stored in the *process environment block* so it can be accessed in user space.
- The windows subsystem process (Csrss: client/server run time subsystem) maintains a parallel data structure for each process that is executing a Windows program. The kernel-mode part of the Windows subsystem (Win32k.sys) also maintains a per-process data structure.
- Compare with the Linux approach of representing processes and threads both with a task structure.
MS Windows process/thread data structures

- Process environment
- Thread environment block
- Executive block
- Windows process block
- Handle table
- Executive process block
- Executive thread block
Microsoft Windows Bootup Process

Smss: Session Manager SubSystem
MS Windows process tree

<table>
<thead>
<tr>
<th>Process</th>
<th>CPU</th>
<th>Private Bytes</th>
<th>Working Set</th>
<th>PID</th>
<th>Description</th>
<th>Company Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Idle Process</td>
<td>76.76</td>
<td>0 K</td>
<td>24 K</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>2.26</td>
<td>128 K</td>
<td>772 K</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interrupts</td>
<td>6.98</td>
<td>0 K</td>
<td>0 K</td>
<td>n/a</td>
<td>Hardware Interrupts and DPCs</td>
<td></td>
</tr>
<tr>
<td>smss.exe</td>
<td>0.32</td>
<td>448 K</td>
<td>1,116 K</td>
<td>360</td>
<td></td>
<td></td>
</tr>
<tr>
<td>csrss.exe</td>
<td>&lt; 0.01</td>
<td>2,672 K</td>
<td>4,824 K</td>
<td>428</td>
<td></td>
<td></td>
</tr>
<tr>
<td>csrss.exe</td>
<td>0.32</td>
<td>11,432 K</td>
<td>7,792 K</td>
<td>468</td>
<td></td>
<td></td>
</tr>
<tr>
<td>conhost.exe</td>
<td>1.164</td>
<td>3,244 K</td>
<td>2,652 K</td>
<td>2652 Console Window Host</td>
<td>Microsoft Corporation</td>
<td></td>
</tr>
<tr>
<td>conhost.exe</td>
<td>2.428</td>
<td>9,204 K</td>
<td>3428 Console Window Host</td>
<td>Microsoft Corporation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wininit.exe</td>
<td>1.498</td>
<td>4,328 K</td>
<td>476</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>services.exe</td>
<td>5.280</td>
<td>9,072 K</td>
<td>576</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lsass.exe</td>
<td>0.01</td>
<td>5,108 K</td>
<td>11,972 K</td>
<td>584</td>
<td>Local Security Authority Process</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>winlogon.exe</td>
<td>2.516</td>
<td>4,212 K</td>
<td>592</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>explorer.exe</td>
<td>1.83</td>
<td>60,789 K</td>
<td>88,392 K</td>
<td>2220 Windows Explorer</td>
<td>Microsoft Corporation</td>
<td></td>
</tr>
<tr>
<td>vmtoolsd.exe</td>
<td>4.68</td>
<td>16,796 K</td>
<td>26,888 K</td>
<td>2992 VMware Tools Core Service</td>
<td>VMware, Inc.</td>
<td></td>
</tr>
<tr>
<td>sidebar.exe</td>
<td>0.01</td>
<td>16,320 K</td>
<td>38,328 K</td>
<td>2816 Windows Desktop Gadgets</td>
<td>Microsoft Corporation</td>
<td></td>
</tr>
<tr>
<td>ONEHENOTEM.EXE</td>
<td>1.044</td>
<td>1,084 K</td>
<td>2852 Microsoft Office OneNote Quick L...</td>
<td>Microsoft Corporation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mssecexe</td>
<td>6,168</td>
<td>17,388 K</td>
<td>3172 Microsoft Security Client User Inter...</td>
<td>Microsoft Corporation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>proceexp.exe</td>
<td>2.280</td>
<td>7,604 K</td>
<td>3012 Sysinternals Process Explorer</td>
<td>Sysinternals - <a href="http://www.sysinternals">www.sysinternals</a>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>proceexp64.exe</td>
<td>2.83</td>
<td>14,304 K</td>
<td>32,516 K</td>
<td>4320 Sysinternals Process Explorer</td>
<td>Sysinternals - <a href="http://www.sysinternals">www.sysinternals</a>...</td>
<td></td>
</tr>
<tr>
<td>devenv.exe</td>
<td>96,984</td>
<td>138,140 K</td>
<td>2072 Microsoft Visual Studio 2012</td>
<td>Microsoft Corporation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chrome.exe</td>
<td>37,096</td>
<td>66,304 K</td>
<td>3488 Google Chrome</td>
<td>Google Inc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>chrome.exe</td>
<td>0.01</td>
<td>17,756 K</td>
<td>13,520 K</td>
<td>3464 Google Chrome</td>
<td>Google Inc.</td>
<td></td>
</tr>
<tr>
<td>chrome.exe</td>
<td>&lt; 0.01</td>
<td>22,516 K</td>
<td>22,184 K</td>
<td>4828 Google Chrome</td>
<td>Google Inc.</td>
<td></td>
</tr>
<tr>
<td>powershell.exe</td>
<td>40,228</td>
<td>48,660 K</td>
<td>2660 Windows PowerShell</td>
<td>Microsoft Corporation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vim.exe</td>
<td>2,528</td>
<td>10,528 K</td>
<td>3396 Vi Improved - A Text Editor</td>
<td>Vim Developers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>gvim.exe</td>
<td>2,532</td>
<td>10,548 K</td>
<td>1144 Vi Improved - A Text Editor</td>
<td>Vim Developers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VCD Daemon.exe</td>
<td>1,536</td>
<td>5,720 K</td>
<td>3632 Virtual CloneDrive Daemon</td>
<td>Elaborate Bytes AG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITunesHelper.exe</td>
<td>&lt; 0.01</td>
<td>3,700 K</td>
<td>11,540 K</td>
<td>3640 ITunesHelper</td>
<td>Apple Inc.</td>
<td></td>
</tr>
<tr>
<td>UA.exe</td>
<td>0.01</td>
<td>34,408 K</td>
<td>37,292 K</td>
<td>3820</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Screenshot of `procexp` program from Sysinternals tools.
A process state diagram is used to characterize the behavior of a process.

A process may be *ready*, *running* or *blocked*. How does the process state change?

The ready and blocked states can be refined to *Active* and *Suspended*. 
Simple Process State Diagram

- Ready
- Blocked
- Start
- Running
- Done

Arrows indicate transitions: request, schedule.
Extended Process State Diagram

- Running
- Done
- Ready Active
- Ready Suspended
- Blocked Active
- Blocked Suspended
- Start

Transitions:
- Request
- Suspend
- Activate
- Yield
- Schedule
- Allocate
See the file `include/linux/sched.h` for the process states defined in the kernel.
MS Windows process states

- **Init (0)**: Used internally while the thread is being created
- **Ready (1)**: A thread in the ready state is waiting to execute
- **Running (2)**: Running on a processor until the quantum ends, it is preempted, it terminates, it yields or it voluntarily enters the wait state
- **Standby (3)**: A thread in the standby state has been selected to run on a particular processor. Only one thread can be in a standby state for each processor on the system. Threads can be preempted from this state
- **Terminated (4)**: In the terminated state, the executive thread block might or might not be deallocated depending on the policy that is set
Waiting (5): A thread can enter the waiting state in several ways: it can voluntarily wait for an object to synchronize its execution, the operating system can wait on its behalf (such as for paging I/O), or it can be suspended by an external entity.

Transition (6): A thread is ready for execution but its kernel stack is paged out of memory.

Deferred Ready (7): Threads that have been selected to run on a specific processor but have not yet been scheduled. This is so that the kernel can minimize the amount of time the systemwide lock on the scheduling database is held.

Gate Waiting (8): When thread does a wait on a gate dispatcher object (separate from the waiting state). Because gates don’t use the dispatcher lock, but a per object lock, the kernel needs to be able to distinguish it if it has to break the lock.
Resources

A process manager also manages resources used by processes.

- A **resource** is anything that can block a process from executing. Examples include: memory, messages, input data, disks, tapes, files etc

- A resource that can be allocated and must be returned after the process has finished are called **reusable resources**. These kind of resources are fixed in number. What if a process does not release reusable resources?

- A resource that is never released is called a **consumable resource**. These kind of resources are unbounded

- Different resource allocation strategies. Give more responsibilities to client processes. E.g. user level threads, IBM virtual machine operating system, virtual machine servers, client-server operating systems and microkernels
Summary

- Executable file formats: creation, loading and running executables
- Memory hierarchy as related to processes
- The process abstraction: How to keep track of processes?
- Process state diagrams