Outline for Today

- Objective:
  - Assignment 2 Rant
  - Continue message passing through ports
  - Unix process-oriented system calls
- Administrative details:
  - Contributions?

Guidelines for Choosing Lock Granularity

1. **Keep critical sections short.** Push “noncritical” statements outside of critical sections to reduce contention.
2. **Limit lock overhead.** Keep to a minimum the number of times mutexes are acquired and released.
   - Note tradeoff between contention and lock overhead.
3. **Use as few mutexes as possible, but no fewer.**
   - Choose lock scope carefully: if the operations on two different data structures can be separated, it may be more efficient to synchronize those structures with separate locks.
   - Add new locks only as needed to reduce contention.
4. **Correctness first, performance second!**

Bad Example

Let us count the ways…

```
Condition::Signal (Lock * conditionLock)
{ // Lock is held on way in...
P (signalMutex);
    thread=(Thread *) queue->Remove();
V (signalMutex);
if (thread != NULL)
    scheduler->ReadyToRun (thread);
}
```

```
Condition::Wait (Lock * conditionLock)
{ // Lock is held on way in...
P (waitMutex);
    queue->Append (currentThread);
V (waitMutex);
    currentThread->Sleep ();
}
```

Naming Destinations for Messages: Ports

It may be useful for a given process to manage multiple communication endpoints — often called ports — with messages sent to ports rather than processes.

```
while systemActive |
    svc->receiveRequest();
    replyport->receive(response);
    svc->send(request);
    replyport->send(response);
```
Advantages of Ports

1. Ports decouple IPC endpoints from processes and threads.
   A thread may send to a port without knowing the identity of the
   process/thread that receives on that port.
   Different threads may listen/service the same port, possibly at
   different times.
2. A thread may listen to multiple ports, separating the
   message streams designated for different ports.
   E.g., assign different ports to different object/virtual services.
3. Ports are a convenient granularity to control message flow.
   E.g., selectively enable/disable ports independently, or assign
   different priorities or access control to different ports.

Port Issues

1. Asynchrony and notification. How does a thread know when a
   message arrives on a port?
   How to receive from multiple ports, without blocking on an idle port
   while incoming messages are queued on another?
2. Naming and binding. How do threads name the ports to send
   to or receive from (listen)?
   How do threads find the names, e.g., for services they want to use?
3. Protection and access control.
   How does the system know if a thread/process has a "right" to send
   to or listen on a particular port? E.g., how can we prevent
   untrusted programs from masquerading as a legitimate service?

Examples of Ports in Real Systems

1. Unix sockets and TCP/IP communication.
   • Common primitives/protocols for local messaging and network
     communication.
   • TCP/IP defines a fixed space of port numbers per node.
     System calls to send/listen to a particular port.
   • Some ports are reserved to processes running with superuser
     (root) privilege.
     Standard servers in /dev/services listen at well-known ports.
2. Mach supplies a rich set of port/messaging primitives.
   • Open ports (port rights) are kernel object handles.
   • Port rights may be passed in messages among processes.
   The only way to get a send/receive right is for some other process to
     pass it to you! This is a system-wide basis for protection.

Notification of Pending Messages

Communication-oriented systems face an important problem:
How does a client or server know what to do next?
• Servers in networks or server-structured systems might service
  many clients, possibly on different ports.
• The server must handle messages as they arrive, without blocking
  to receive on an empty port while others have pending messages.

Option 1: Use blocking primitives with lots of threads.
Leave the scheduling to the thread scheduler.

Option 2: Introduce nonblocking primitives or provide
notifications or combined queueing of incoming messages.
A wide variety of mechanisms have been used: nonblocking
polling, Unix select, Mach port groups, event queues, etc.
Polling: Select

A thread/process with multiple network connections or open files can initiate nonblocking I/O on all of them.

- The Unix `select` system call supports such a polling model:
  - pass a bitmask for which descriptors to query for readiness
  - returns a bitmask of descriptors ready for reading/writing
  - reads and/or writes on these descriptors will not block.

Immediate Notification: Upcalls

**Problem:** what if an event requires a more “immediate” notification?

- What if a high-priority event occurs while we are executing the handler for a low-priority event?
- What about exceptions relating to the handling of an event?

We need some way to preemptively “break in” to the execution of a thread and notify it of events.

- **Polling**
  - example: NT Asynchronous Procedure Calls (APCs)
  - example: Unix signals
  - Preemptive event handling raises synchronization issues similar to interrupt handling

---

**Lock Service with RPC**

```java
while (true)
    receiveRequest(msg);
    if (msg.op == acquire)
        Lock->Acquire();
    if (msg.op == release)
        Lock->Release();
    if (msg.op == newlock) ...
```

**Lock Service with Send/Receive**

```java
while (true)
    receiveRequest(msg);
    if (msg.op == acquire)
        LockServer->Send(acquire, lock);
        LockServer->Receive(OKmsg);
    if (msg.op == release)
        LockServer->Send(release, lock);
        LockServer->Receive(OKmsg);
    if (msg.op == newlock) ...
```
Lock Service with Ports

**P₀**
- LockServerPort = Send (newLock,ReplyPort)
- ReplyPort = Receive (OKmsg)

**P₁**
- LockPort = Send (acquire,ReplyPort)
- ReplyPort = Receive (OKmsg)
- C.S.
- LockPort = Send (release,ReplyPort)
- ReplyPort = Receive (OKmsg)

Advantages of Server “Isolation” Afforded by Message Passing

Like the kernel, the server is protected from its clients.
- Address space isolation is preserved, so the client cannot corrupt the server’s data.
- The only way a client can cause code to run in the server is to send a message.
  The server decides how to validate and interpret each message.
  (Unlike the kernel, the server cannot access client memory.)
- The client is also protected from the server, although it must rely on it to correctly perform the service.

Protected servers may coordinate interactions among processes, manage system-critical data, or otherwise assume roles “typically” reserved for the operating system kernel.

Reconsidering the Kernel Interface and OS Structure

The kernel can be thought of as nothing more than a server; it is special only in that it runs in a protected hardware mode.
- Many of the services traditionally offered by the kernel can be supported outside of the kernel, in servers or in libraries.
- What features must be implemented in the kernel? Could we implement (say) the entire Unix interface as an application?
- Why would we want to do such a thing?
  What are the advantages of supporting some OS feature in a server rather than directly in the kernel? What are the costs?
- How would we design a kernel interface that is powerful enough to implement multiple OS “personalities” as servers?

*The kernel interface is not the programming interface!*

Servers and Microkernels

A number of systems have been structured as collections of servers running above a minimal kernel ("microkernel").
- Microkernel provides, e.g., basic thread and scheduling, IPC, virtual address spaces, and device I/O primitives.
  Kernel is hoped to be smaller, more reliable, and more secure.
  Policies (e.g., security) may be implemented outside of the kernel.
- Operating system “personalities” (e.g., Unix or Windows) may be implemented as servers.
  OS may have multiple personalities and policies, with new OS features and APIs added on-the-fly.
- The performance of server-structured systems is determined largely by the efficiency of the messaging primitives.
Microkernel with “User-Level” OS Server Processes

Boundary Crossings?

Unix Process Model

- Simple and powerful primitives for process creation and initialization.
  - `fork` syscall creates a child process as (initially) a clone of the parent
  - parent program runs in child process to set it up for `exec`
  - child can `exit`, parent can `wait` for child to do so.
- Rich facilities for controlling processes by asynchronous signals:
  - notification of internal and/or external events to processes or groups
  - the look, feel, and power of interrupts and exceptions
  - default actions: stop process, kill process, dump core, no effect
  - user-level handlers

Unix Process Control

- Child process waits until the child's parent is ready
- Parent waits for its children to complete

End-to-End Argument

- Application-level correctness requires checking at the endpoints to ensure that the message exchange accomplished its purpose
  - Application semantics involved
  - Notification of successful delivery (UPS tracking) is not as good as a direct response (thank you note) from the other end.
- Reliability guarantees in the message-passing subsystem provide performance benefits (short-circuiting corrective measures).
  - Re-transmitting packet may save re-transferring whole file.
Child Discipline

- After a fork, the parent program (not process) has complete control over the behavior of its child process.
- The child inherits its execution environment from the parent...but the parent program can change it.
  - sets bindings of file descriptors with open, close, dup
  - pipe sets up data channels between processes
- Parent program may cause the child to execute a different program, by calling exec* in the child context.

Exec, Execve, etc.

- Children should have lives of their own.
- Exec* “boots” the child with a different executable image.
  - parent program makes exec* syscall (in forked child context) to run a program in a new child process
  - exec* overlays child process with a new executable image
  - restarts in user mode at predetermined entry point (e.g., _crt0)
  - no return to parent program (it’s gone)
  - arguments and environment variables passed in memory
  - file descriptors etc. are unchanged

Fork/Exit/Wait Example

OS resources
fork
parent
fork
child
wait
exit

Child process starts as clone of parent, sharing resources.
Parent and child execute independently: memory states and resources may diverge.
On exit, release memory and decrement refcounts on shared resources.
Child enters zombie state: process is dead and most resources are released, but process descriptor remains until parent reaps exit status via wait.
Parent sleeps in wait until child stops or exits.

Fork/Exec/Exit/Wait Example

int pid = fork();
Create a new process that is a clone of its parent.

exec("program", &argv, &envp);
Overlay the calling process virtual memory with a new program, and transfer control to it.

exit(status);
Exit with status, destroying the process.

int pid = wait(&status);
Wait for exit (or other status change) of a child.
Join Scenarios

- Several cases must be considered for join (e.g., exit/wait).
  - What if the child exits before the parent joins?
    - “Zombie” process object holds child status and stats.
  - What if the parent continues to run but never joins?
    - Danger of filling up memory with zombie processes?
  - Parent might have specified it was not going to wait or that it would ignore its child’s exit. Child status can be discarded.
  - What if the parent exits before the child?
    - Orphans become children of init (process 1).
  - What if the parent can’t afford to get “stuck” on a join?
    - Asynchronous notification (we’ll see an example later).

Unix Signals

- Signals notify processes of internal or external events.
  - the Unix software equivalent of interrupts/exceptions
  - only way to do something to a process “from the outside”
  - Unix systems define a small set of signal types
- Examples of signal generation:
  - keyboard <ctrl>-c and <ctrl>-z signal the foreground process
  - synchronous fault notifications, syscall errors
  - asynchronous notifications from other processes via kill
  - IPC events (SIGPIPE, SIGCHLD)
  - alarm notifications

Process Handling of Signals

1. Each signal type has a system-defined default action.
   - abort and dump core (SIGSEGV, SIGBUS, etc.)
   - ignore, stop, exit, continue
2. A process may choose to **block** (inhibit) or **ignore** some signal types.
3. The process may choose to **catch** some signal types by specifying a (user mode) **handler** procedure.
   - specify alternate signal stack for handler to run on
   - system passes interrupted context to handler
   - handler may munge and/or return to interrupted context

User’s View of Signals

```c
int alarmflag = 0;  
alarmHandler()  
{  printf("An alarm clock signal was received
");  alarmflag = 1;  }  
main()  
{  signal(SIGALRM, alarmHandler);  
  alarm(3); printf("Alarm has been set
");  
  while (!alarmflag ) pause();  
  printf("Back from alarm signal handler
");  }  
```

- Suspends caller until signal
- Sets up signal handler
- Instructs kernel to send SIGALRM in 3 seconds
- Instructs kernel to send SIGALRM in 3 seconds
- Instructs kernel to send SIGALRM in 3 seconds
Yet Another User’s View

```c
main(argc, argv)
int argc; char* argv[];
{
    pid = fork();
    if (pid == 0) /*child*/
        execvp (argv[2], & argv[2]);
    else
        sleep (5);
        printf("child too slow 
");
        kill (pid, SIGINT);
}
```

```
childhandler()
int childPid, childStatus;
childPid = wait (& childStatus);
printf("child done in time!
");
exit;
```

SIGCHLD sent by child on termination; if SIG_IGN, dezombie

Files (& everything else)

- **Descriptors** are small unsigned integers used as handles to manipulate objects in the system, all of which resemble files.
- **open** with the name of a file returns a descriptor
- **read** and **write**, applied to a descriptor, operate at the current position of the file offset. **seek** reposes it.
- Pipes are unnamed, unidirectional I/O stream created by **pipe**.
- Devices are special files, created by **mknod**, with **ioctl** used for parameters of specific device.
- Sockets introduce 3 forms of **sendmsg** and 3 forms of **recvmsg** syscalls.

File Descriptors

- Unix processes name I/O and IPC objects by integers known as **file descriptors**.
  - File descriptors 0, 1, and 2 are reserved by convention for standard **input**, standard **output**, and standard **error**.
  - “Conforming” Unix programs read input from **stdin**, write output to **stdout**, and errors to **stderr** by default.
  - Other descriptors are assigned by syscalls to open/create files, create pipes, or bind to devices or network sockets.
    - **pipe**, **socket**, **open**, **creat**
  - A common set of syscalls operate on open file descriptors independent of their underlying types.
    - **read**, **write**, **dup**, **close**

File System Calls
main(int argc, char *argv[]) {
   char c;
    int fdrd, fdwt;
    if ((fdrd = open(argv[1], O_RDONLY)) == -1)
        exit(1);
    if ((fdwt = creat(argv[2], 0666)) == -1)
        exit(1);
    fork();
    for (;;) {
        if (read(fdrd, &c, 1) != 1)
            exit(0);
        write(fdwt, &c, 1);
    }
}

File Sharing Between Parent/Child

Sharing Open File Instances

Producer/Consumer Pipes

Pipes support a simple form of concurrency with built-in flow control.

while (inbytes != 0) {
    inbytes = read(stdin, inbuffer, 1024);
    outbytes = process data from inbuffer to outbuffer;
    write(outbuffer, outbytes);
}

e.g. sort <grades | grep Dan | mail nadia

Setting Up Pipelines

int pfd[2] = {0, 0}; /* pfd[0] is read, pfd[1] is write */
in = pfd[0]; /* pipeline entrance */
out = pfd[1]; /* pipeline exit */
/* loop to create a child and add it to the pipeline */
for (i = 1; i < procCount; i++) { /* pipeline is a producer/consumer bounded buffer */
    out = setup_child(out);
}
/* pipeline is a producer/consumer bounded buffer */
write(in, ..., ...);
read(out, ..., ...);
Setting Up a Child in a Pipeline

```c
int setup_child(int rfd) {
    int pfd[2] = {0, 0}; /* pfd[0] is read, pfd[1] is write */
    int i, wfd;

    pipe(pfd); /* create right-hand pipe */
    wfd = pfd[1]; /* this child's write side */
    if (fork()) { /* parent */
        close(wfd); close(rfd);
    } else { /* child */
        close(pfd[0]); /* close far end of right pipe */
        close(0); /* stdin */ close(1); /* stdout */
        dup(rfd); /* takes fd 0 */ dup(wfd); /* takes fd 1 */
        close(rfd); close(wfd);
    }
    return(pfd[0]);
}
```

Sockets for Client-Server Message Passing

**Server**
1. Create a named socket syscalls: `sfd = (socket, ...)`
2. Listen for clients `bind(sfd, ...)`
3. Connection made and continue listening `cfd=accept(sfd, ...)`
4. Exchange data `write(cfd, ...)`
5. Exchange data `read(cfd, ...)`
6. Done: close(cfd); close(sfd);

**Client**
1. Create unnamed socket & ask for connection syscalls: `cfd=socket(...) err=connect(cfd, ptr, ...)`
2. Connection made `cfd=accept(sfd, ...)`
3. Exchange data `write(cfd, ...)`
4. Exchange data `read(cfd, ...)`
5. Done: close(cfd);