CS 33

Signals Part 1
Whoops ...

$ SometimesUsefulProgram xyz
Are you sure you want to proceed? Y
Are you really sure? Y
Reformatting of your disk will begin in 3 seconds.
Everything you own will be deleted.
There's little you can do about it.
Too bad ...

Oh dear...
A Gentler Approach

- Signals
  - get a process’s attention
    » send it a signal
  - process must either deal with it or be terminated
    » in some cases, the latter is the only option
Stepping Back …

• What are we trying to do?
  – interrupt the execution of a program
    » cleanly terminate it
    or
    » cleanly change its course

  – not for the faint of heart
    » it's difficult
    » it gets complicated
    » (not done in Windows)
Signals

- **Generated (by OS) in response to**
  - exceptions (e.g., arithmetic errors, addressing problems)
    » synchronous signals
  - external events (e.g., timer expiration, certain keystrokes, actions of other processes)
    » asynchronous signals
- **Effect on process:**
  - termination (possibly producing a core dump)
  - invocation of a function that has been set up to be a signal handler
  - suspension of execution
  - resumption of execution

Signals are a kernel-supported mechanism for reporting events to user code and forcing a response to them. There are actually two sorts of such events, to which we sometimes refer as *exceptions* and *interrupts*. The former occur typically because the program has done something wrong. The response, the sending of a signal, is immediate; such signals are known as *synchronous* signals. The latter are in response to external actions, such as a timer expiring, an action at the keyboard, or the explicit sending of a signal by another process. Signals send in response to these events can seemingly occur at any moment and are referred to as *asynchronous* signals.

Processes react to signals using the actions shown in the slide. The action taken depends partly on the signal and partly on arrangements made in the process beforehand.
This slide shows the complete list of signals required by POSIX 1003.1, the official Unix specification. In addition, many Unix systems support other signals, some of which we’ll mention in the course. The third column of the slide lists the default actions in response to each of the signals. *term* means the process is terminated, *core* means there is also a core dump; *ignore* means that the signal is ignored; *stop* means that the process is stopped (suspended); *cont* means that a stopped process is resumed (continued); *forced* means that the default action cannot be changed and that the signal cannot be blocked or ignored.
Note that the signals generated by typing control characters on the keyboard are actually sent to the current process group of the terminal, a concept we discuss soon.
Handling Signals

```c
#include <signal.h>

typedef void (*sighandler_t)(int);
sighandler_t signal(int signo,
        sighandler_t handler);

sighandler_t OldHandler;

OldHandler = signal(SIGINT, NewHandler);
```
Special Handlers

- **SIGIGN**
  - ignore the signal
  - `signal(SIGINT, SIG_IGN);`

- **SIG_DFL**
  - use the default handler
    - usually terminates the process
    - `signal(SIGINT, SIG_DFL);`
Example

```c
int main() {
    void handler(int);

    signal(SIGINT, handler);
    while(1)
    {
        return 1;
    }
    void handler(int signo) {
        printf("I received signal %d. "
            "Whooppe!!\n", signo);
    }
}
```

Note that the C compiler implicitly concatenates two adjacent strings, as done in printf above.
The `sigaction` system call is the more general means for establishing a process’s response to a particular signal. Its first argument is the signal for which a response is being specified, the second argument is a pointer to a `sigaction` structure defining the response, and the third argument is a pointer to memory in which a `sigaction` structure will be stored containing the specification of what the response was prior to this call. If the third argument is null, the prior response is not returned.

The `sa_handler` member of `sigaction` is either a pointer to a user-defined handler function for the signal or one of SIG_DFL (meaning that the default action is taken) or SIG_IGN (meaning that the signal is to be ignored). The `sigaction` member is an alternative means for specifying a handler function; we discuss it in an upcoming slide.

When a user-defined signal-handler function is entered in response to a signal, the signal itself is masked until the function returns. Using the `sa_mask` member, one can specify additional signals to be masked while the handler function is running. On return from the handler function, the process’s previous signal mask is restored.

The `sa_flags` member is used to specify various other things which we describe in upcoming slides.
Example

```c
int main() {
    void handler(int);
    struct sigaction act;
    act.sa_handler = handler;
    sigemptyset(&act.sa_mask);
    act.sa_flags = 0;
    sigaction(SIGINT, &act, 0);

    while(1)
    {
        return 1;
    }

    void handler(int signo) {
        printf("I received signal %d. "
               "Whoopee!!\n", signo);
    }
}
```

This has behavior identical to the previous example; we’re using `sigaction` rather than `signal` to set up the signal handler.
Quiz 1

```c
int main() {
    void handler(int);
    struct sigaction act;
    act.sa_handler = handler;
    sigemptyset(&act.sa_mask);
    act.sa_flags = 0;
    sigaction(SIGINT, &act, NULL);

    while(1)
        ;
    return 1;
}

void handler(int signo) {
    printf("I received signal %d. ", signo);
    if (signo == SIGINT) {
        printf("Whoopee!!!\n");
        return;
    }
}
```

You run the example program, then quickly type ctrl-C. What is the most likely explanation if the program then terminates?

a) you’re really quick or the system is really slow
b) this “can’t happen;” thus there’s a problem with the system
c) there’s something else going on we haven’t yet explained
The “FPE” SIGFPE stands for floating-point exception, but that’s an artifact from the early days of UNIX. Any arithmetic exception generates a SIGFPE.
The slide illustrates the signature of the handler procedure used with `siginfo`, as well as a partial example of its use. The third parameter is a pointer to a structure of type `ucontext_t` and contains the register context of the process at the time of interruption by the signal. We won't be discussing it further in this course, but information about its use can be found in the man page for `ucontext`.

The `siginfo` structure (of type `siginfo_t`) has a large number of fields. The slide illustrates how one can use it to determine the kind of arithmetic error that just occurred. See the man page for `sigaction` for discussion of everything that can be determined from the `siginfo` structure. (It won't be used in this course.)
Here we use the `setitimer` system call to arrange so that a SIGALRM signal is generated in one millisecond. (The system call takes three arguments: the first indicates how time should be measured; what’s specified here is to use real time. See its man page for other possibilities. The second argument contains a `struct itimerval` that itself contains two `struct timeval`s. One (named `it_value`) indicates how much time should elapse before a SIGALRM is generated for the process. The other (named `it_interval`), if non-zero, indicates that a SIGALRM should be sent again, repeatedly, every `it_interval` period of time. Each process may have only one pending timer, thus when a process calls `setitimer`, the new value replaces the old. If the third argument to `setitimer` is non-zero, the old value is stored at the location it points to.)

The `pause` system call causes the process to block and not resume until some signal that is not ignored is delivered.
This program is guaranteed to print “success!”.

a) yes
b) no

signal(SIGALRM, RespondToSignal);

...

struct timeval waitperiod = {0, 1000};
    /* seconds, microseconds */
struct timeval interval = {0, 0};
struct itimerval timerval;
timerval.it_value = waitperiod;
timerval.it_interval = interval;

setitimer(ITIMER_REAL, &timerval, 0);
    /* SIGALRM sent in ~one millisecond */
pause(); /* wait for it */
printf("success!\n");
Masking Signals

```c
setitimer(ITIMER_REAL, &timerval, 0);
   /* SIGALRM sent in ~one millisecond */

No signals here, please!

pause();    /* wait for it */
```
Masking Signals

mask SIGALRM
setitimer(ITIMER_REAL, &timerval, 0);
    /* SIGALRM sent in ~one millisecond */

No signals here

unmask and wait for SIGALRM
Here’s a safer way of doing what was attempted in the earlier slide. We mask the SIGALRM signal before calling `setitimer`. Then, rather than calling `pause`, we call `sigsuspend`, which sets the set of masked signals to its argument and, at the same instant, blocks the calling process. Thus if the SIGALRM is generated before our process calls `sigsuspend`, it won’t be delivered right away. Since the call to `sigsuspend` reinstates the previous mask (which, presumably, did not include SIGALRM), the SIGALRM signal will be delivered and the process will return (after invoking the handler). When `sigsuspend` returns, the signal mask that was in place just before it was called is restored. Thus we have to restore `oldset` explicitly.

As with `pause`, `sigsuspend` returns only if an unmasked signal that is not ignored is delivered.
Signal Sets

- To clear a set:
  ```c
  int sigemptyset(sigset_t *set);
  ```

- To add or remove a signal from the set:
  ```c
  int sigaddset(sigset_t *set, int signo);
  int sigdelset(sigset_t *set, int signo);
  ```

- Example: to refer to both SIGHUP and SIGINT:
  ```c
  sigset_t set;

  sigemptyset(&set);
  sigaddset(&set, SIGHUP);
  sigaddset(&set, SIGINT);
  ```

A number of signal-related operations involve sets of signals. These sets are normally represented by a bit vector of type `sigset_t`.
In addition to ignoring signals, you may specify that they are to be blocked (that is, held pending or masked). When a signal type is masked, signals of that type remains pending and do not interrupt the process until they are unmasked. When the process unblocks the signal, the action associated with any pending signal is performed. This technique is most useful for protecting critical code that should not be interrupted. Also, as we’ve already seen, when the handler for a signal is entered, subsequent occurrences of that signal are automatically masked until the handler is exited, hence the handler never has to worry about being invoked to handle another instance of the signal it’s already handling.
Signal Handlers and Masking

• What if a signal occurs while a previous instance is being handled?
  – inconvenient ...

• Signals are masked while being handled
  – may mask other signals as well:

```c
struct sigaction act; void myhandler(int);
sigemptyset(&act.sa_mask); // zeroes the mask
sigaddset(&act.sa_mask, SIGQUIT);
  // also mask SIGQUIT
act.sa_flags = 0;
act.sa_handler = myhandler;
sigaction(SIGINT, &act, NULL);
```
This slide sketches something that one might want to try to do: give a user a limited amount of time (in this case, 30 seconds — the `alarm` routine causes the system to send the process a SIGALRM signal in the given number of seconds) to provide some input, then, if no input, notify the caller that there is a problem. Here we’d like our timeout handler to transfer control to someplace else in the program, but we can’t do this. (Note also that we should cancel the call to `alarm` if there is input. So that we can fit all the code in the slide, we’ve left this part out.)
To get around the problem of not being able to use a goto statement to get out of a signal handler, we introduce the setjmp/longjmp facility, also known as the nonlocal goto. A call to sigsetjmp stores context information (about the current locus of execution) that can be restored via a call to siglongjmp. A bit more precisely: sigsetjmp stores into its first argument the values of the program-counter (instruction-pointer), stack-pointer, and other registers representing the process’s current execution context. If the second argument is non-zero, the current signal mask is saved as well. The call returns 0. When siglongjmp is called with a pointer to this context information as its first argument, the current register values are replaced with those that were saved. If the signal mask was saved, that is restored as well. The effect of doing this is that the process resumes execution where it was when the context information was saved: inside of sigsetjmp. However, this time, rather than returning zero, it returns the second argument passed to siglongjmp (1 in the example).

To use this facility, you must include the header file setjmp.h.
The effect of `sigsetjmp` is to save the registers relevant to the current stack frame; in particular, the instruction pointer, the frame pointer (if used), and the stack pointer, as well as the return address and the current signal mask. A subsequent call to `siglongjmp` restores the stack to what it was at the time of the call to `sigsetjmp`. Note that `siglongjmp` should be called only from a stack frame that is farther on the stack than the one in which `sigsetjmp` was called.
Exceptions

- Other languages support exception handling

```java
try {
    something_a_bit_risky();
} catch (ArithmeticException e) {
    deal_with_it(e);
}
```

- Can we do something like this in C?
The slide suggests a C syntax for exception handling. The TRY/CATCH/END behave as the try/catch does in the previous slide. The signal handler responds to exceptions, then THROWs the exception, to be caught in the TRY/CATCH/END construct. The big question, of course, is can we implement this?
Here’s an implementation of TRY, CATCH, END, and THROW using macros. Note that since #define statements are restricted to one line, we “escape” the ends of lines with back slashes.
And here is the code with the macros expanded.