Unix Programming

Process and Signal

Overview

1. What is a Process?
2. `fork()`
3. `exec()`
4. `wait()`
5. Process Data
6. File Descriptors across Processes
7. Special Exit Cases
8. IO Redirection
9. User/Group ID real and effective
10. getenv/putenv, ulimit()

1. What is a Process?

- **A process is an executing program.**
- **A process:**

```
$ cat file1 file2 &
```

- **Two processes:**

```
$ ls | wc - l
```

- **Each user can run many processes at once (e.g. using `&`)**

A More Precise Definition

- **A process is the *context* (the information/ data) maintained for an executing program.**
- **Intuitively, a process is the abstraction of a physical processor.**
  - Exists because it is difficult for the OS to otherwise coordinate many concurrent activities, such as incoming network data, multiple users, etc.
- **IMPORTANT: A process is sequential**

What makes up a Process?

- **program code**
- **machine registers**
- **global data**
- **stack**
- **open files (file descriptors)**
- **an environment (environment variables; credentials for security)**

Some of the Context Information

- Process ID (`pid`) — unique integer
- Parent process ID (`ppid`)
- Real User ID — ID of user/process which started this process
- Effective User ID — ID of user who wrote the process' program
- Current directory
- File descriptor table
- Environment — `VAR=VALUE` pairs

continued

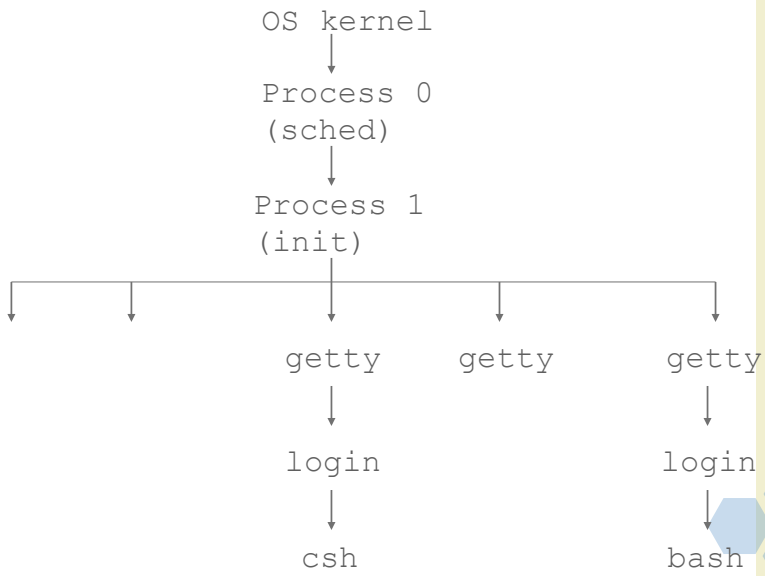
- Pointer to program code
- Pointer to data — Memory for global vars
- Pointer to stack — Memory for local vars
- Pointer to heap — Dynamically allocated

- Execution priority
- Signal information

Important System Processes

- **init – Mother of all processes. init is started at boot time and is responsible for starting other processes.**
  - init uses file inittab & directories: /etc/rc?.d
- **getty – login process that manages login sessions.**

Unix Start Up Processes Diagram



Pid and Parentage

- **A process ID or *pid* is a positive integer that uniquely identifies a running process, and is stored in a variable of type *pid_t*.**
- **You can get the process pid or parent's pid**

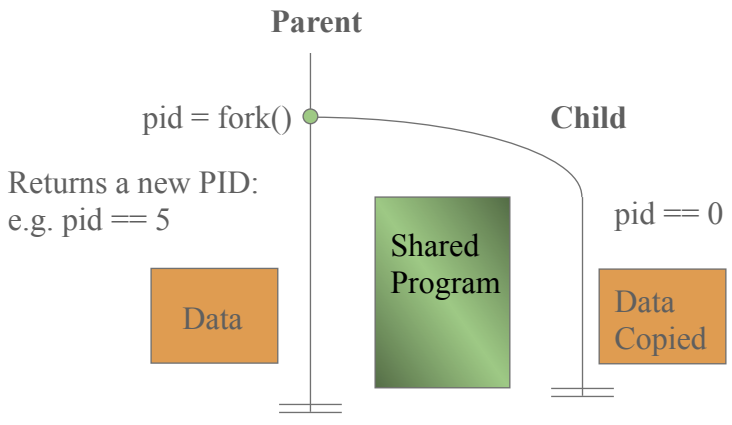
```
#include <sys/types>
main()
  {
  pid_t pid, ppid;
  printf( "My  PID is:%d\n\n",(pid = getpid()) );
  printf( "Par PID is:%d\n\n",(ppid = getppid()) );
  }
```

2. fork()

```
#include <sys/types.h>
#include <unistd.h>
pid_t fork( void );
```

- **Creates a child process by making a copy of the parent process --- an exact duplicate.**
  - Implicitly specifies code, registers, stack, data, files
- **Both the child *and* the parent continue running.**

fork() as a diagram



Process IDs (pids revisited)

- `pid = fork();`
- **In the child:** `pid == 0`**;**
  In the parent: `pid` **== the process ID of the child.**
- **A program almost always uses this** `pid` **difference to do different things in the parent and child.**

fork() Example (parchld.c)

```
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>

int main()
{
    pid_t pid;          /* could be int */
    int i;
    pid = fork();
    if( pid > 0 )
    {
          /* parent */
          for( i=0; i < 1000; i++ )
                printf("\t\t\tPARENT %d\n", i);
    }
```

```
else
     {
     /* child */
     for( i=0; i < 1000; i++ )
           printf( "CHILD %d\n", i );
     }
   return 0;
 }
```

Possible Output

```
CHILD 0
CHILD 1
CHILD 2
                PARENT 0
                PARENT 1
                PARENT 2
                PARENT 3
CHILD 3
CHILD 4
                PARENT 4
          :
```

Things to Note

- `i` is copied between parent and child.
- The switching between the parent and child depends on many factors:
  - machine load, system process scheduling
- I/O buffering effects amount of output shown.
- Output interleaving is *nondeterministic*
  - cannot determine output by looking at code

3. exec()

- Family of functions for replacing process's program with the one inside the `exec()` call.
  e.g.

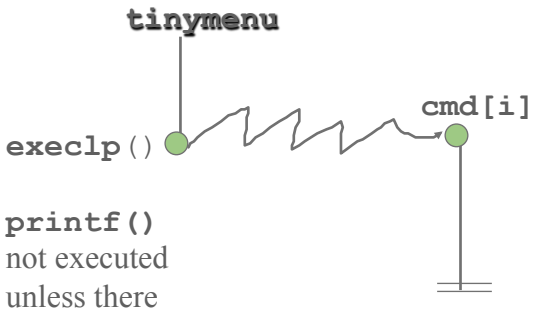
```
#include <unistd.h>
int execlp(char *file, char *arg0,
        char *arg1, ..., (char *)0);

execlp("sort", "sort", "-n",
                "foobar", (char *)0);
```

Same as "sort -n foobar"

tinymenu.c

```
#include <stdio.h>
#include <unistd.h>

void main()
{ char *cmd[] = {"who", "ls", "date"};
  int i;
  printf("0=who 1=ls 2=date : ");
  scanf("%d", &i);

  execlp( cmd[i], cmd[i], (char *)0 );
  printf( "execlp failed\n" );
}
```

Execution



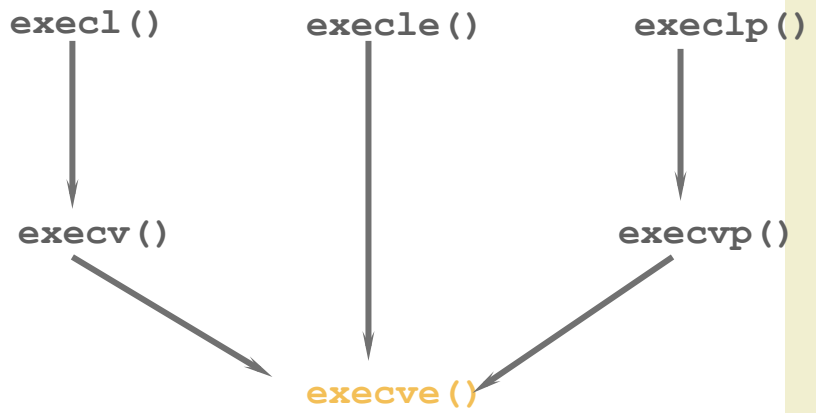
printf() not executed unless there is a problem with **execlp()**

exec(..) Family

- **There are 6 versions of the exec function, and they all do about the same thing: they replace the current program with the text of the new program. Main difference is how parameters are passed.**

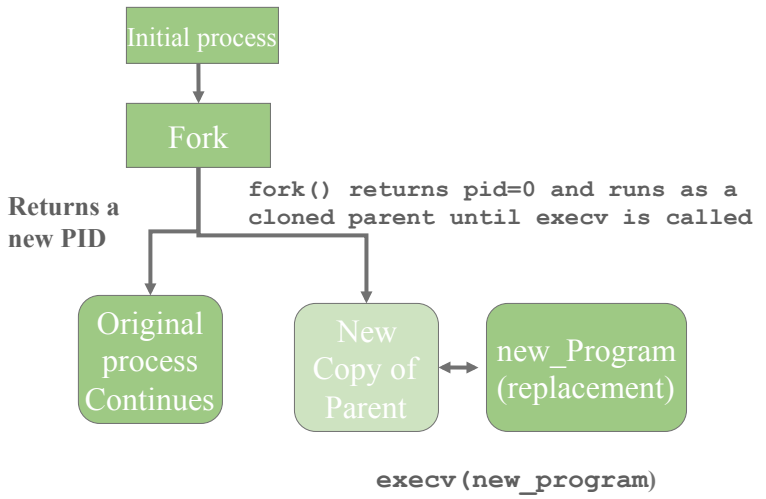
```
int execl( const char *path, const char *arg, ... );
int execlp( const char *file, const char *arg, ... );
int execle( const char *path, const char *arg
          , ..., char *const envp[] );
int execv( const char *path, char *const argv[] );
int execvp( const char *file, char *const argv[] );
int execve( const char *filename, char *const argv [],
char *const envp[] );
```

exec(..) Family



fork() and execv()

- `execv(new_program, argv[ ])`



4. wait()

```
#include <sys/types.h>
#include <sys/wait.h>
pid_t wait(int *statloc);
```

- **Suspends calling process until child has finished. Returns the process ID of the terminated child if ok, -1 on error.**
- **`statloc` can be `(int *)0` or a variable which will be bound to status info. about the child.**

wait() Actions

- **A process that calls `wait()` can:**
  - *suspend* (block) if all of its children are still running, or
  - *return* immediately with the *termination* status of a child, or
  - *return* immediately with an *error* if there are no child processes.

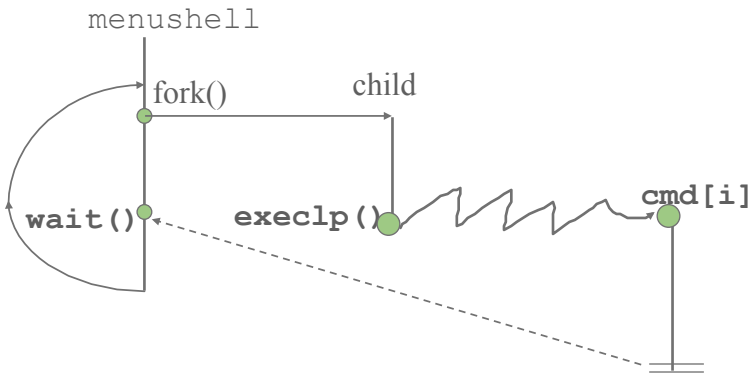
menushell.c

```
#include <stdio.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/wait.h>

void main()
{
    char *cmd[] = {"who", "ls", "date"};
    int i;
    while( 1 )
          {
          printf( 0=who 1=ls 2=date : " );
          scanf( "%d", &i );
               :
```

continued

```
if(fork() == 0)
    {  /* child */
    execlp( cmd[i], cmd[i], (char *)0 );
    printf( "execlp failed\n" );
    exit(1);
    }
else
    {  /* parent */
    wait( (int *)0 );
    printf( "child finished\n" );
    }
  } /* while */
} /* main */
```

Execution



Macros for wait (1)

- **WIFEXITED(*status*)**
  - Returns true if the child exited normally.
- **WEXITSTATUS(*status*)**
  - Evaluates to *the least significant eight bits* of the return code of the child which terminated, which may have been set as the argument to a call to exit( ) or as the argument for a return.
  - This macro can only be evaluated if WIFEXITED returned non-zero.

Macros for wait (2)

- **WIFSIGNALED(*status*)**
  - Returns true if the child process exited *because of a signal* which was not caught.
- **WTERMSIG(*status*)**
  - Returns *the signal number* that caused the child process to terminate.
  - This macro can only be evaluated if WIFSIGNALED returned non-zero.

waitpid()

```
#include <sys/types.h>
#include <sys/wait.h>
pid_t waitpid( pid_t pid, int *status, int opts )
```

- **waitpid - can wait for a particular child**
- ***pid* < -1**
  - Wait for any child process whose process group ID is equal to the absolute value of *pid*.
- ***pid* == -1**
  - Wait for any child process.
  - Same behavior which wait( ) exhibits.
  - *pid* == 0
  - Wait for any child process whose process group ID is equal to that of the calling process.

- ***pid* > 0**
  - Wait for the child whose process ID is equal to the value of *pid*.
  - *options*
    - Zero or more of the following constants can be ORed.
      - WNOHANG
        - » Return immediately if no child has exited.
      - WUNTRACED
        - » Also return for children which are stopped, and whose status has not been reported (because of signal).
  - Return value
    - The process ID of the child which exited.
    - -1 on error; 0 if WNOHANG was used and no child was available.

Macros for waitpid

- **WIFSTOPPED(*status*)**
  - Returns true if the child process which caused the return is *currently stopped*.
  - This is only possible if the call was done using WUNTRACED.
- **WSTOPSIG(status)**
  - Returns *the signal number* which caused the child to stop.
  - This macro can only be evaluated if WIFSTOPPED returned non-zero.

Example: waitpid

```
#include <stdio.h>
#include <sys/wait.h>
#include <sys/types.h>

int main(void)
   {
   pid_t pid;
   int status;

   if( (pid = fork() ) == 0 )
       { /* child */
       printf("I am a child with pid = %d\n",
       getpid());
       sleep(60);
       printf("child terminates\n");
       exit(0);
       }
```

```
else
    { /* parent */
      while (1)
      {
          waitpid( pid, &status, WUNTRACED );
          if( WIFSTOPPED(status) )
          {
                  printf("child stopped, signal(%d)\n",
                         WSTOPSIG(status));
                  continue;
              }
          else if( WIFEXITED(status) )
                  printf("normal termination with
                      status(%d)\n",
                      WEXITSTATUS(status));
          else if (WIFSIGNALED(status))
                  printf("abnormal termination,
                      signal(%d)\n",
                      WTERMSIG(status));
          exit(0);
          } /* while */
    } /* parent */
} /* main */
```

5. Process Data

- **Since a child process is a copy of the parent, it has copies of the parent's data.**
- **A change to a variable in the child will *not* change that variable in the parent.**

Example (globex.c)

```
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>

int globvar = 6;
char buf[] = "stdout write\n";

int main(void)
 {
    int w = 88;
    pid_t pid;
```

continued

```
    write( 1, buf, sizeof(buf)-1 );
    printf( "Before fork()\n" );

    if( (pid = fork()) == 0 ) {  /* child */
       globvar++;
       w++;
    }
    else if( pid > 0 )        /* parent */
       sleep(2);
    else
       perror( "fork error" );

    printf( "pid = %d, globvar = %d, w = %d\n",
          getpid(), globvar, w );
    return 0;
} /* end main */
```

Output

```
$ globex
stdout write      /* write not buffered */

Before fork()
pid = 430, globvar = 7, w = 89
                  /*child chg*/
pid = 429, globvar = 6, w = 88
                  /* parent no chg */
```

```
$ globex > temp.out
$ cat temp.out
stdout write
Before fork()
pid = 430, globvar = 7, w = 89
Before fork() /* fully buffered */
pid = 429, globvar = 6, w = 88
```

6. Process File Descriptors

- **A child and parent have copies of the file descriptors, but the R-W pointer is maintained by the system:**
  - the R-W pointer is shared
- **This means that a `read()` or `write()` in one process will affect the other process since the R-W pointer is changed.**

Example: File used across processes

(shfile.c)

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/wait.h>
#include <unistd.h>
#include <fcntl.h>
void printpos(char *msg, int fd);
void fatal(char *msg);

int main(void)
{ int fd;    /* file descriptor */
  pid_t pid;
  char buf[10]; /* for file data */
    :
```

continued

```
if ((fd=open("data-file", O_RDONLY)) < 0)
   perror("open");

   read(fd, buf, 10);  /* move R-W ptr */

   printpos( "Before fork", fd );

   if( (pid = fork()) == 0 )
        {  /* child */
        printpos( "Child before read", fd );
        read( fd, buf, 10 );
        printpos( " Child after read", fd );
        }
        :
```

continued

```
else if( pid > 0 )
   {    /* parent */
   wait((int *)0);
   printpos( "Parent after wait", fd );
   }
else
   perror( "fork" );
}
```

continued

```
void printpos( char *msg, int fd )
/* Print position in file */
    {
    long int pos;

    if( (pos = lseek( fd, 0L, SEEK_CUR) ) < 0L )
         perror("lseek");

    printf( "%s: %ld\n", msg, pos );
    }
```

Output

```
$ shfile

Before fork: 10
Child before read: 10
Child after read: 20
Parent after wait: 20
```

what's happened?

8. Special Exit Cases

Two special cases:

- **1) A child exits when its parent is not currently executing `wait()`**
  - the child becomes a *zombie*
  - `status` data about the child is stored until the parent does a `wait()`

continued

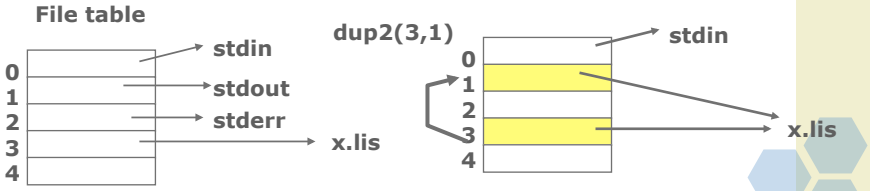
- **2) A parent exits when 1 or more children are still running**
  - children are adopted by the system's initialization process (`/etc/init`)
    - it can then monitor/kill them

9. I/O redirection

- **The trick: you can change where the standard I/O streams are going/ coming from after the fork but before the exec**

Redirection of standard output

- **Example implement shell: ls > x.ls**
- **program:**
  - Open a new file x.lis
  - Redirect standard output to x.lis using **dup** command
    - everything sent to standard output ends in x.lis
  - execute ls in the process
- **dup2(int fin, int fout) - copies fin to fout in the file table**



Example - implement ls > x.lis

```
#include <unistd.h>
int main ()
  {
  int fileId;
  fileId = creat( "x.lis",0640 );
  if( fileId < 0 )
      {
      printf( stderr, "error creating x.lis\n" );
      exit (1);
      }
  dup2( fileId, stdout ); /* copy fileID to stdout */
  close( fileId );
  execl( "/bin/ls", "ls", 0 );
  }
```

10. User and Group ID

- **Group ID**
  - Real, effective
- **User ID**
  - Real user ID
    - Identifies the user who is responsible for the running process.
  - Effective user ID
    - Used to assign ownership of newly created files, to check file access permissions, and to check permission to send signals to processes.
    - To change euid: executes a *setuid-program* that has the set-uid bit set or invokes the setuid( ) system call.
    - The setuid(*uid*) system call: if euid is not superuser, *uid* must be the real uid or the saved uid (the kernel also resets euid to *uid*).
  - Real and effective uid: inherit (fork), maintain (exec).

Read IDs

- **pid_t getuid(void);**
  - Returns the real user ID of the current process
- **pid_t geteuid(void);**
  - Returns the effective user ID of the current process
- **gid_t getgid(void);**
  - Returns the real group ID of the current process
- **gid_t getegid(void);**
  - Returns the effective group ID of the current process

Change UID and GID (1)

```
#include <unistd.h>
#include <sys/types.h>
int setuid( uid_t uid )
int setgid( gid_t gid )
```

- **Sets the effective user ID of the current process.**
  - Superuser process resets the real effective user IDs to *uid*.
  - Non-superuser process can set effective user ID to *uid*, only when *uid* equals real user ID or the saved set-user ID (set by executing a setuid-program in exec).
  - In any other cases, setuid returns error.

Change UID and GID (2)

ID	exec		setuid(uid)	
	suid bit off	suid bit on	superuser	other users
real-uid	unchanged	unchanged	uid	unchanged
effective-uid	unchanged	set from user ID of program file	uid	uid
saved set-uid	copied from euid	copied from euid	uid	unchanged

Change UID and GID (3)

```
#include <unistd.h>
#include <sys/types.h>
int setreuid( uid_t ruid, uid_t euid )
```

- Sets real and effective user ID's of the current process.
- Un-privileged users may change the real user ID to the effective user ID and vice-versa.
- It is also possible to set the effective user ID from the saved user ID.
- Supplying a value of -1 for either the real or effective user ID forces the system to leave that ID unchanged.
- If the real user ID is changed or the effective user ID is set to a value not equal to the previous real user ID, the saved user ID will be set to the new effective user ID.

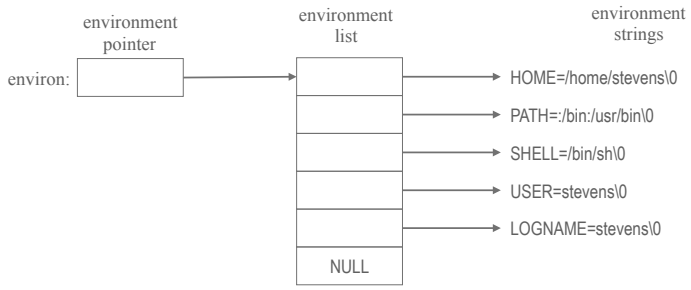
Change UID and GID (4)

- int seteuid(uid_t *euid*);
  - seteuid(*euid*) is functionally equivalent to setreuid(-1, *euid*).
  - Setuid-root program wishing to temporarily drop root privileges, assume the identity of a non-root user, and then regain root privileges afterwards cannot use setuid, because setuid issued by the superuser changes all three IDs. One can accomplish this with seteuid.
- int setregid(gid_t *rgid*, gid_t *egid*);
- int setegid(gid_t *egid*);

11. Environment

extern char **environ;

int main(int *argc*, char **argv[ ]*, char **envp[ ]*)



Example: environ

```
#include <stdio.h>

void main( int argc, char *argv[], char *envp[] )
   {
   int i;
   extern char **environ;

   printf( "from argument envp\n" );

   for( i = 0; envp[i]; i++ )
       puts( envp[i] );

   printf("\nFrom global variable environ\n");

   for( i = 0; environ[i]; i++ )
           puts(environ[i]);
}
```

getenv

- **#include <stdlib.h>**

  char *getenv(const char *_name_);
  - Searches the environment list for a string that matches the string pointed to by *name*.
  - Returns a pointer to the value in the environment, or NULL if there is no match.

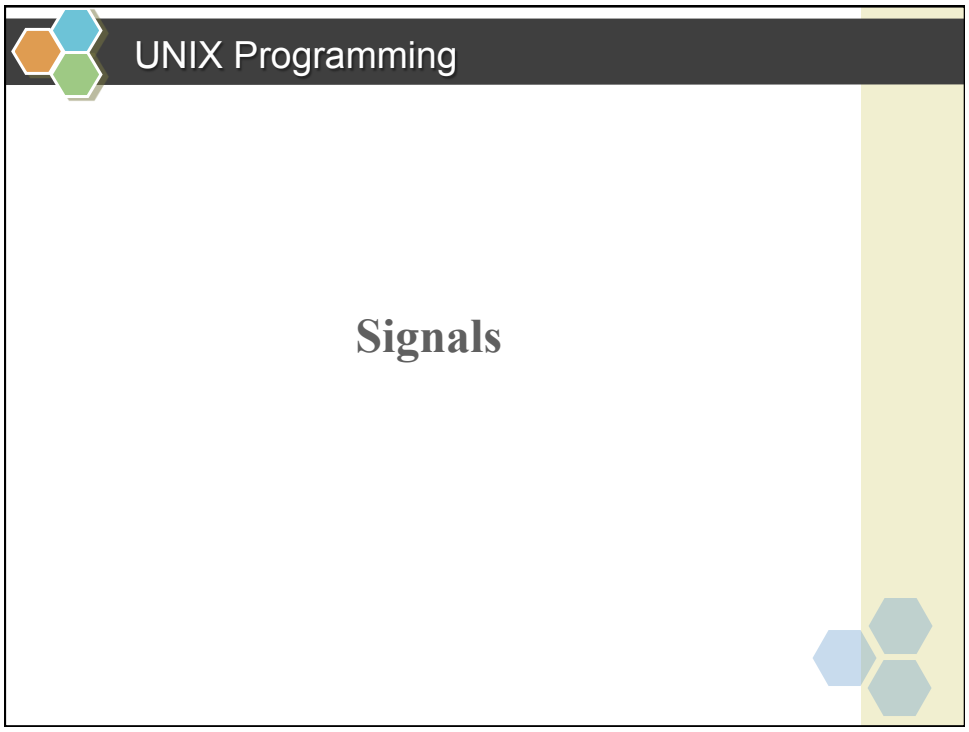
putenv

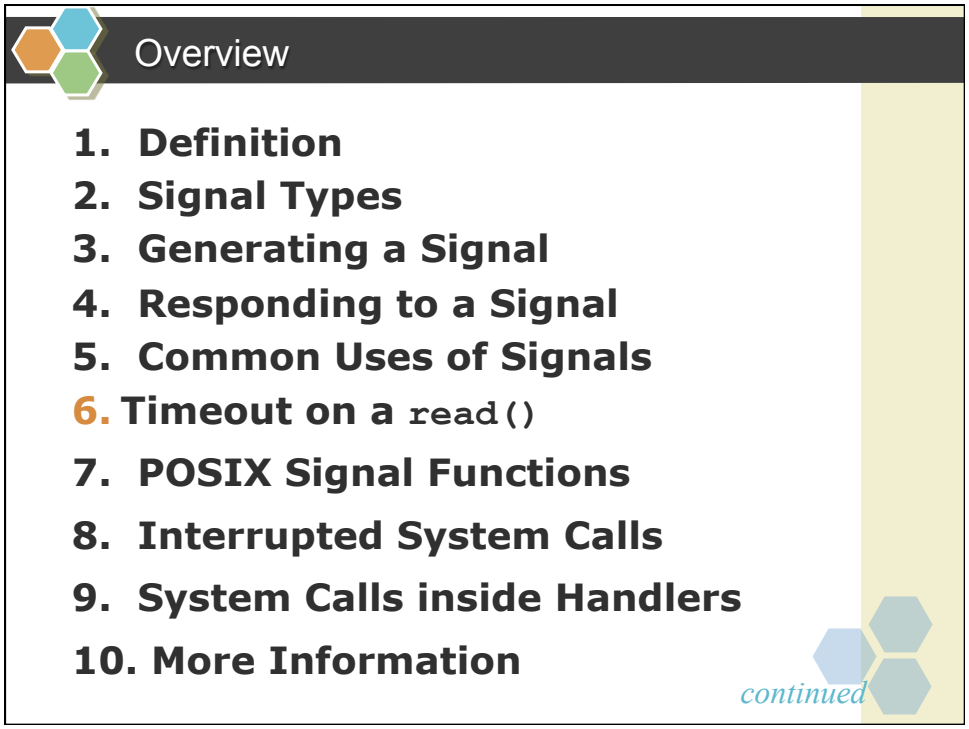
- **#include <stdlib.h>**

  int putenv(const char *_string_);
  - Adds or changes the value of environment variables.
  - The argument *string* is of the form name=value.
  - If name does not already exist in the environment, then string is added to the environment.
  - If name does exist, then the value of name in the environment is changed to value.
  - Returns zero on success, or -1 if an error occurs.

Example : getenv, putenv

```
#include <stdio.h>
#include <stdlib.h>

void main(void)
{
    printf("Home directory is %s\n", getenv("HOME"));

    putenv("HOME=/");

    printf("New home directory is %s\n", getenv("HOME"));
}
```


UNIX Programming
Signals


Overview
1. Definition
2. Signal Types
3. Generating a Signal
4. Responding to a Signal
5. Common Uses of Signals
6. Timeout on a read()
7. POSIX Signal Functions
8. Interrupted System Calls
9. System Calls inside Handlers
10. More Information
continued

1. Definition

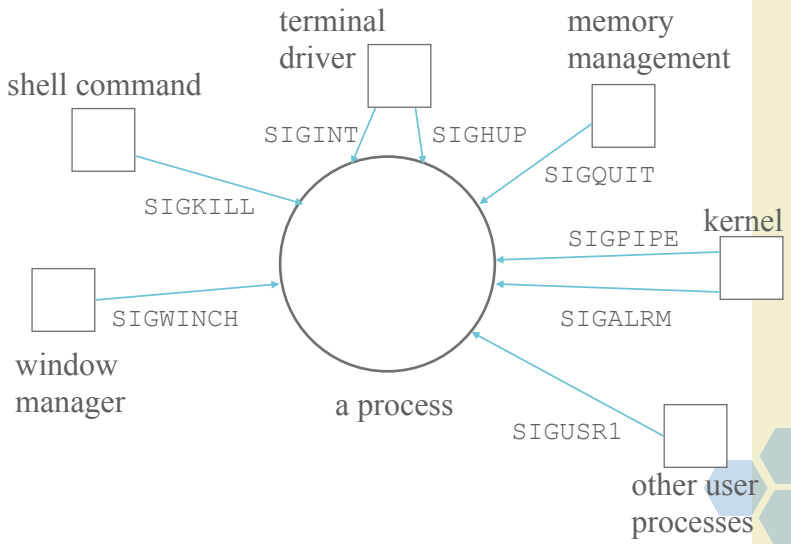
- **A signal is an *asynchronous* event which is delivered to a process.**
- **Asynchronous means that the event can occur at any time**
  - may be unrelated to the execution of the process
  - e.g. user types `ctrl-C`, or the modem hangs

2. Signal Types (31 in POSIX)

Name	*Description*	*Default Action*
`SIGINT`	Interrupt character typed	terminate process
`SIGQUIT`	Quit character typed (`^\`)	create core image
`SIGKILL`	`kill -9`	terminate process
`SIGSEGV`	Invalid memory reference	create core image
`SIGPIPE`	Write on pipe but no reader	terminate process
`SIGALRM`	`alarm()` clock 'rings'	terminate process
`SIGUSR1`	user-defined signal type	terminate process
`SIGUSR2`	user-defined signal type	terminate process

- **See** `man 7 signal`

Signal Sources



3. Generating a Signal

- **Use the UNIX command:**

```
$ kill -KILL 4481
```

  - send a `SIGKILL` signal to pid 4481
  - check
    - `ps -l`
  - to make sure process died

- **`kill` is not a good name; `send_signal` might be better.**

kill()

- **Send a signal to a process (or group of processes).**
- `#include <signal.h>`

  `int kill( pid_t pid, int signo );`
- **Return 0 if ok, -1 on error.**

Some pid Values

pid	*Meaning*
> 0	**send signal to process `pid`**
== 0	**send signal to all processes whose process group ID equals the sender's pgid. e.g. parent kills all children**

4. Responding to a Signal

- **A process can:**
  - ignore/discard the signal (not possible with `SIGKILL` or `SIGSTOP`)
  - execute a signal handler function, and then possibly resume execution or terminate
  - carry out the default action for that signal
- **The choice is called the process' *signal disposition***

signal(): library call

- **Specify a signal handler function to deal with a signal type.**
-
```
#include <signal.h>
typedef void Sigfunc(int);  /* my defn */

Sigfunc *signal( int signo, Sigfunc *handler );
```
  - signal returns a pointer to a function that returns an int (i.e. it returns a pointer to Sigfunc)
- **Returns *previous* signal disposition if ok, `SIG_ERR` on error.**

Actual Prototype

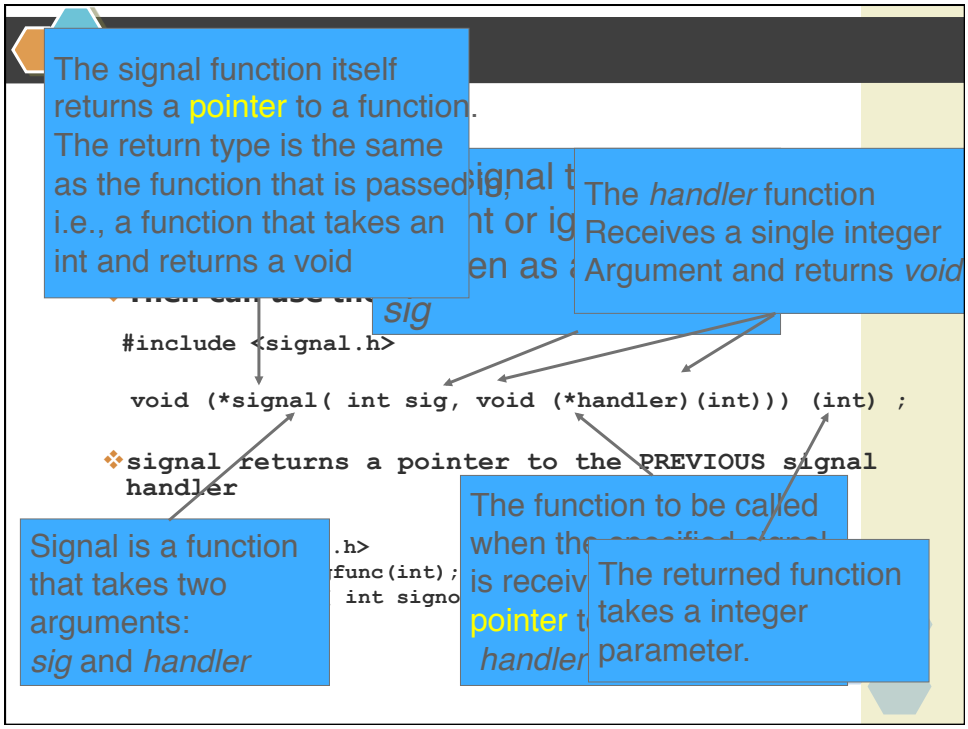
- **The actual prototype, listed in the "man" page is a bit perplexing but is an expansion of the `Sigfunc` type:**

```
void (*signal(int signo, void(*handler)(int)))(int);
```

- **In Linux:**

```
typedef void (*sighandler_t)(int);

sig_handler_t signal(int signo, sighandler_t handler);
```

- **Signal returns a pointer to a function that returns an int**



Example

```
int main()
    {
    signal( SIGINT, foo );
      :

    /* do usual things until SIGINT */
    return 0;
    }

void foo( int signo )
    {
      :          /* deal with SIGINT signal */


    return;      /* return to program */
    }
```

sig_examp.c

```
#include <stdio.h>
#include <unistd.h>
#include <signal.h>

void sig_usr( int signo );    /* handles two signals */

int main()
  {
  int i = 0;
  if( signal( SIGUSR1,sig_usr ) == SIG_ERR )
      printf( "Cannot catch SIGUSR1\n" );
  if( signal( SIGUSR2,sig_usr ) == SIG_ERR )
     printf("Cannot catch SIGUSR2\n");
                :
```

continued

```
        :
  while(1)
        {
        printf( "%2d\n", I );
        pause();
        /* pause until signal handler
         * has processed signal */
        i++;
        }
  return 0;
}
```

continued

```
void sig_usr( int signo )
/* argument is signal number */
{
  if( signo == SIGUSR1 )
        printf("Received SIGUSR1\n");
  else if( signo == SIGUSR2 )
        printf("Received SIGUSR2\n");
  else
        printf("Error: received signal
                %d\n", signo);

  return;
}
```

Usage

```
$ sig_examp &
[1]      4720
 0
$ kill -USR1 4720
Received SIGUSR1
 1
$ kill -USR2 4720
Received SIGUSR2
 2
$ kill 4720            /* send SIGTERM */
[1] + Terminated    sig_examp &
$
```


Special Sigfunc * Values

Value	*Meaning*
`SIG_IGN`	**Ignore / discard the signal.**
`SIG_DFL`	**Use default action to handle signal.**
`SIG_ERR`	**Returned by `signal()` as an error.**

Multiple Signals

- **If many signals of the *same* type are waiting to be handled (e.g. two `SIGINT`s), then most UNIXs will only deliver one of them.**
  - the others are thrown away
- **If many signals of *different* types are waiting to be handled (e.g. a `SIGINT`, `SIGSEGV`, `SIGUSR1`), they are not delivered in any fixed order.**

pause()

- **Suspend the calling process until a signal is caught.**
- `#include <unistd.h>`
  `int pause(void);`
- **Returns -1 with `errno` assigned `EINTR`. (Linux assigns it `ERESTARTNOHAND`).**
- `pause()` **only returns after a signal handler has returned.**

The Reset Problem

- **In Linux (and many other UNIXs), the signal disposition in a process is reset to its default action immediately after the signal has been delivered.**
- **Must call `signal()` again to reinstall the signal handler function.**

Reset Problem Example

```
int main()
    {
    signal(SIGINT, foo);
     :
    /* do usual things until SIGINT */
    }

void foo(int signo)
    {
    signal(SIGINT, foo); /* reinstall */
          :
    return;
    }
```

Reset Problem

```
     :
void ouch( int sig )
       {
       printf( "OUCH! - I got signal %d\n", sig );
       (void) signal(SIGINT, ouch);
       }
int main()
       {
       (void) signal( SIGINT,
       while(1)
              {
              printf("Hello World!\n");
              sleep(1);
              }
       }
```

To keep catching the signal with this function, must call the *signal* system call again.

Problem: from the time that the interrupt function starts to just before the signal handler is re-established the signal will not be handled.

If another SIGINT signal is received during this time, default behavior will be done, i.e., program will terminate.

Re-installation may be too slow!

- **There is a (very) small time period in `foo()` when a new `SIGINT` signal will cause the default action to be carried out -- process termination.**
- **With `signal()` there is no answer to this problem.**
  - POSIX signal functions solve it (and some other later UNIXs)

5. Common Uses of Signals

5.1. Ignore a Signal
5.2. Clean up and Terminate
5.3. Dynamic Reconfiguration
5.4. Report Status
5.5. Turn Debugging on/off
5.6. Restore Previous Handler

5.1. Ignore a Signal

```
    :
int main()
{
  signal(SIGINT, SIG_IGN);
  signal(SIGQUIT, SIG_IGN);
    :
  /* do work without interruptions */
}
```

- **Cannot ignore/handle `SIGKILL` or `SIGSTOP`**
- **Should check for `SIG_ERR`**

5.2. Clean up and Terminate

```
    :
/* global variables */
int my_children_pids;
    :
void clean_up(int signo);

int main()
{
  signal(SIGINT, clean_up);
    :
}
```

continued

```
void clean_up(int signo)
{
  unlink("/tmp/work-file");
  kill(my_children_pids,
SIGTERM);
  wait((int *)0);
  fprintf(stderr,
       "Program terminated\n");
  exit(1);
}
```

Problems

- **If a program is run in the background then the interrupt and quit signals (`SIGINT`, `SIGQUIT`) are automatically ignored.**
- **Your code should not override these changes:**
  - check if the signal dispositions are `SIG_IGN`

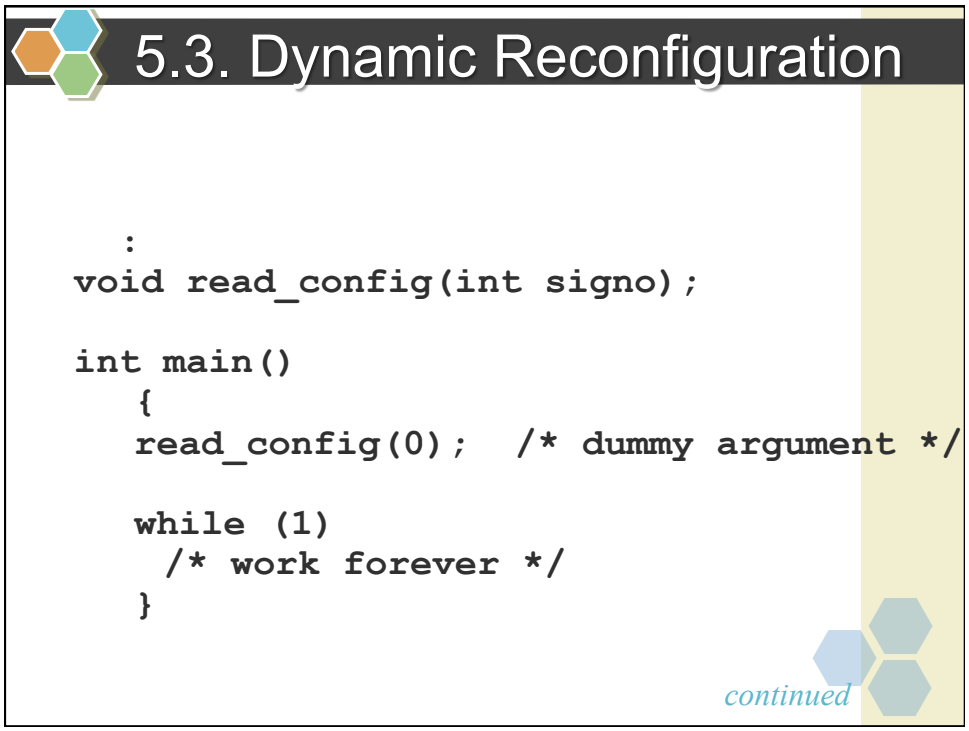
Checking the Disposition

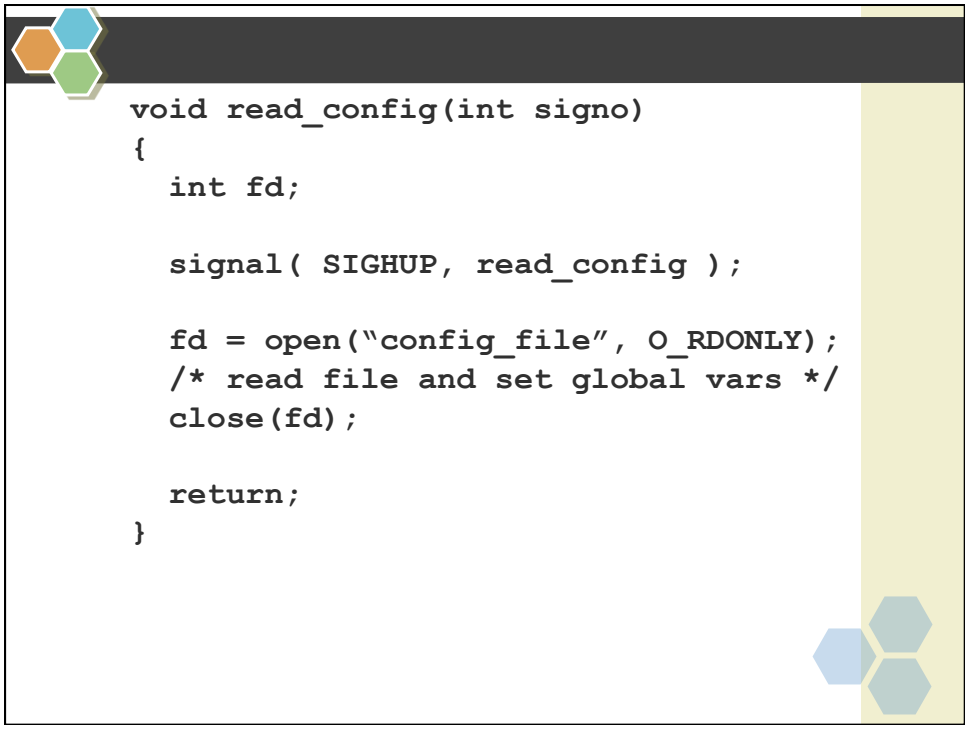
new disposition

old disposition

```
    :
if( signal(SIGINT, SIG_IGN ) != SIG_IGN )
    signal(SIGINT, clean_up);

 if( signal(SIGQUIT, SIG_IGN ) != SIG_IGN )
    signal(SIGQUIT, clean_up);
    :
```

- ***Note*: cannot check the signal disposition without changing it (sigaction that we will look at later , is different)**


5.3. Dynamic Reconfiguration
:
void read_config(int signo);
int main()
{
read_config(0); /* dummy argument */
while (1)
/* work forever */
}
continued


void read_config(int signo)
{
int fd;
signal(SIGHUP, read_config);
fd = open("config_file", O_RDONLY);
/* read file and set global vars */
close(fd);
return;
}

Problems

- **Reset problem**
- **Handler interruption**
  - what is the effect of a `SIGHUP` in the middle of `read_config()`'s execution?
- **Can only affect global variables.**

5.4. Report Status

```
  :
void print_status(int signo);
int count;   /* global */

int main()
{ signal(SIGUSR1, print_status);
   :
  for( count=0; count < BIG_NUM; count++ )
   {
    /* read block from tape */
    /* write block to disk */
   }
  ...
}
```

continued

```
void print_status(int signo)
{
  signal(SIGUSR1, print_status);
  printf("%d blocks copied\n", count);
  return;
}
```

- **Reset problem**
- `count` **value not always defined.**
- **Must use global variables for status information**

5.5. Turn Debugging on/off

```
  :
void toggle_debug(int signo);

int debug = 0;  /* initialize here */

int main()
{
  signal(SIGUSR2, toggle_debug);

  /* do work */
  if (debug == 1)
        printf("...");
  ...
}
```

continued

```
void toggle_debug(int signo)
{
  signal(SIGUSR2, toggle_debug);

  debug = ((debug == 1) ? 0 : 1);

  return;
}
```

5.6. Restore Previous Handler

```
   :
Sigfunc *old_hand;

/* set action for SIGTERM;
   save old handler */
old_hand = signal(SIGTERM, foobar);

/* do work */

/* restore old handler */
signal(SIGTERM, old_hand);
   :
```

6. Implementing a read() Timeout

- **Put an upper limit on an operation that might block forever**
  - e.g. `read()`
- **6.1. `alarm()`**
  6.2. Bad `read()` Timeout
  6.3. `setjmp()` and `longjmp()`
  6.4. Better `read()` Timeout

6.1. alarm()

- **Set an alarm timer that will 'ring' after a specified number of seconds**
  - a `SIGALRM` signal is generated
- **`#include <unistd.h>`**
  `long alarm(long secs);`
- **Returns 0 or number of seconds until previously set alarm would have 'rung'.**

Some Tricky Aspects

- **A process can have at most one alarm timer running at once.**
- **If `alarm()` is called when there is an existing alarm set then it returns the number of seconds remaining for the old alarm, and sets the timer to the new alarm value.**
  - What do we do with the "old alarm value"?
- **An `alarm(0)` call causes the previous alarm to be cancelled.**

6.2. Bad read() Timeout

```
#include <stdio.h>
#include <unistd.h>
#include <signal.h>

#define MAXLINE   512

void sig_alrm( int signo );

int main()
    {
    int n;
    char line[MAXLINE];
         :
```

continued

```
    if( signal(SIGALRM, sig_alrm) == SIG_ERR )
          {
          printf("signal(SIGALRM) error\n");
          exit(1);
          }

    alarm(10);
    n = read( 0, line, MAXLINE );
    alarm(0);

    if( n < 0 )  /* read error */
          fprintf( stderr, "\nread error\n" );
    else
          write( 1, line, n );
    return 0;
}
```

continued

```
void sig_alrm(int signo)
/* do nothing, just handle signal */
{
  return;
}
```

Problems

- **The code assumes that the `read()` call terminates with an error after being interrupted (talk about this later).**
- **Race Conditon: The kernel may take longer than 10 seconds to start the `read()` after the `alarm()` call.**
  - the alarm may 'ring' before the `read()` starts
  - then the `read()` is not being timed; may block forever
  - Two ways two solve this:
    - `setjmp`
    - `sigprocmask` and `sigsuspend`

6.3. setjmp() and longjmp()

- **In C we cannot use `goto` to jump to a label in another function**
  - use `setjmp()` and `longjmp()` for those 'long jumps'
- **Only uses which are good style:**
  - error handling which requires a deeply nested function to recover to a higher level (e.g. back to `main()`)
  - coding timeouts with signals

Prototypes

```
#include <setjmp.h>
int setjmp( jmp_buf env );
```

- **Returns 0 if called directly, non-zero if returning from a call to `longjmp()`.**

```
#include <setjmp.h>
void longjmp( jmp_buf env, int val );
```

Behavior

- **In the `setjmp()` call, `env` is initialized to information about the current state of the stack.**
- **The `longjmp()` call causes the stack to be reset to its `env` value.**
- **Execution restarts after the `setjmp()` call, but this time `setjmp()` returns `val`.**

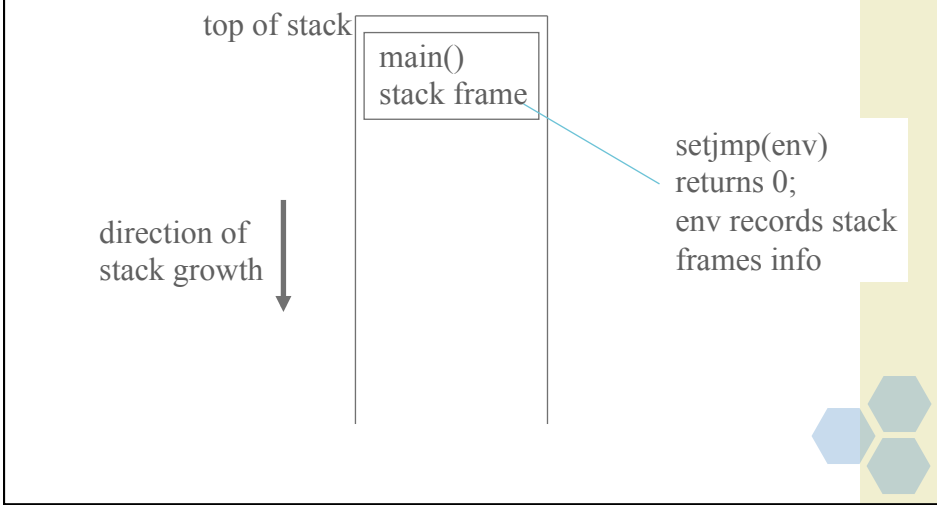
Example

```
    :
jmp_buf env;          /* global */

int main()
    {
    char line[MAX];
    int errval;

    if(( errval = setjmp(env) ) != 0 )
          printf( "error %d: restart\n", errval );

    while( fgets( line, MAX, stdin ) != NULL )
          process_line(line);
    return 0;
    }
```

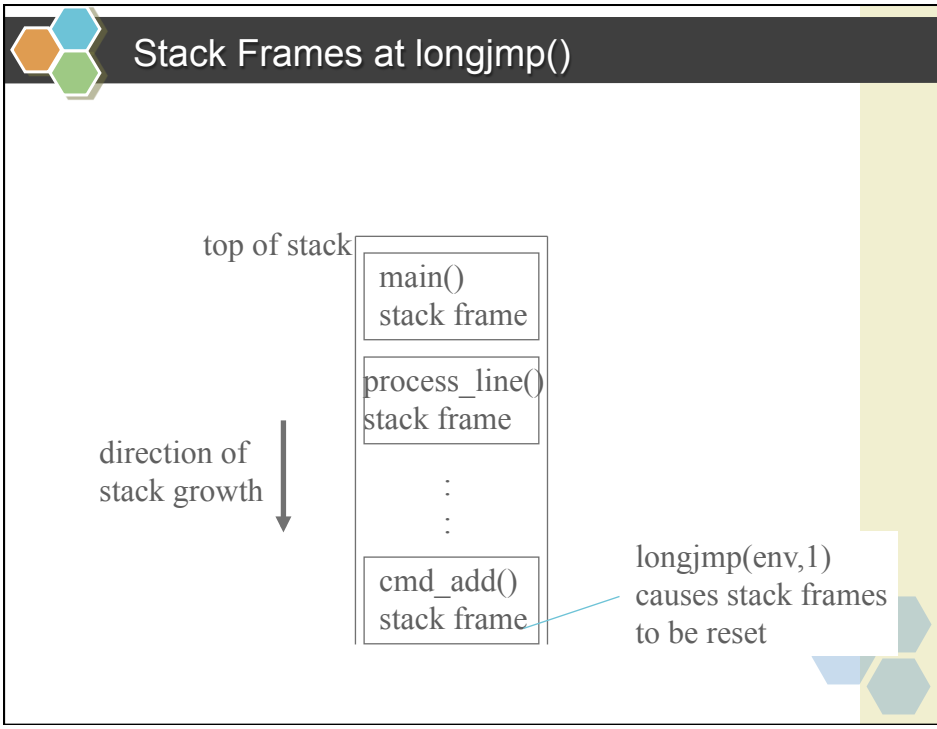
continued

```
    :
void process_line( char * ptr )
    {
    :
    cmd_add()
    :
    }

void cmd_add()
    {
    int token;

    token = get_token();
    if( token < 0 )      /* bad error */
          longjmp( env, 1 );

    /* normal processing */
    }
int get_token()
    {
    if( some error )
          longjmp( env, 2 );
    }
```

Stack Frames at setjmp()



Stack Frames at longjmp()



sleep1()

```
#include <signal.h>
#include <unistd.h>

void sig_alrm( int signo )
     {
     return; /* return to wake up pause */
     }
unsigned int sleep1( unsigned int nsecs )
     {
     if( signal( SIGALRM, sig_alrm ) == SIG_ERR )
            return (nsecs);
     alarm( nsecs );            /* starts timer */
     pause();                   /* next caught signal wakes */
     return( alarm( 0 ) );      /* turn off timer, return unslept
                                 * time */
     }
```

sleep2()

```
static void jmp_buf env_alrm;

void sig_alrm( int signo )
     {
     longjmp( env_alrm, 1 );
     }
unsigned int sleep2( unsigned int nsecs )
     {
     if( signal( SIGALRM, sig_alrm ) == SIG_ERR )
            return (nsecs);
     if( setjmp( env_alrm) == 0 )
            {
            alarm( nsecs );     /* starts timer */
            pause();            /* next caught signal wakes */
            }
     return( alarm( 0 ) );
     }
```

continued

Sleep1 and Sleep2

- **Sleep2 fixes race condition. Even if the pause is never executed.**
- **There is one more problem (will talk about that after "fixing the earlier read function")**

Status of Variables?

- **The POSIX standard says:**
  - global and static variable values will not be changed by the `longjmp()` call
- **Nothing is specified about local variables, are they "rolled back" to their original values (at the setjmp call) as the stack"?**
  - they may be restored to their values at the first `setjmp()`, but maybe not
    - Most implementations do not roll back their values

6.4. Better read() Timeout

```
#include <stdio.h>
#include <unistd.h>
#include <setjmp.h>
#include <signal.h>

#define MAXLINE  512
void sig_alrm( int signo );
jmp_buf env_alrm;

int main()
{ int n;
  char line[MAXLINE];
        :
```

continued

```
if( signal(SIGALRM, sig_alrm) == SIG_ERR)
      {
      printf("signal(SIGALRM) error\n");
      exit(1);
      }

if( setjmp(env_alrm) != 0 )
      {
      fprintf(stderr, "\nread() too slow\n");
      exit(2);
      }

alarm(10);
n = read(0, line, MAXLINE);
alarm(0);
```

continued

```
    if( n < 0 )  /* read error */
          fprintf( stderr, "\nread error\n" );
    else
          write( 1, line, n );
    return 0;
}
```

continued

```
void sig_alrm(int signo)
/* interrupt the read() and jump to
   setjmp() call with value 1
*/
{
  longjmp(env_alrm, 1);
}
```

Caveat: Non-local Jumps

From the UNIX `man` pages:

```
WARNINGS
     If longjmp() or siglongjmp() are called even though env  was
     never  primed  by a call to setjmp() or sigsetjmp(), or when
     the last  such  call  was  in  a  function  that  has  since
     returned, absolute chaos is guaranteed.
```


A Problem Remains!

- **If the program has several signal handlers then:**
  - execution might be inside one when an alarm 'rings'
  - the `longjmp()` call will jump to the `setjmp()` location, and abort the other signal handler -- might lose / corrupt data

7. POSIX Signal Functions

- **The POSIX signal functions can control signals in more ways:**
  - can *block signals* for a while, and deliver them later (good for coding critical sections)
  - can *switch off the resetting* of the signal disposition when a handler is called (no reset problem)

- **The POSIX signal system, uses signal sets, to deal with pending signals that might otherwise be missed while a signal is being processed**

7.1. Signal Sets

- **The signal set stores collections of signal types.**
- **Sets are used by signal functions to define which signal types are to be processed.**
- **POSIX contains several functions for creating, changing and examining signal sets.**

Prototypes

- `#include <signal.h>`

```
int sigemptyset( sigset_t *set );
int sigfillset( sigset_t *set );

int sigaddset( sigset_t *set, int signo );
int sigdelset( sigset_t *set, int signo );

int sigismember( const sigset_t *set,
                                 int signo );
```

7.2. sigprocmask()

- **A process uses a signal set to create a mask which defines the signals it is blocking from delivery. – good for critical sections where you want to block certain signals.**

- `#include <signal.h>`
  `int sigprocmask( int how,`
  `const sigset_t *set,`
  `sigset_t *oldset);`
- `how – indicates how mask is modified`

how Meanings

Value	*Meaning*
`SIG_BLOCK`	`set` **signals are added to mask**
`SIG_UNBLOCK`	`set` **signals are removed from mask**
`SIG_SETMASK`	`set` **becomes new mask**

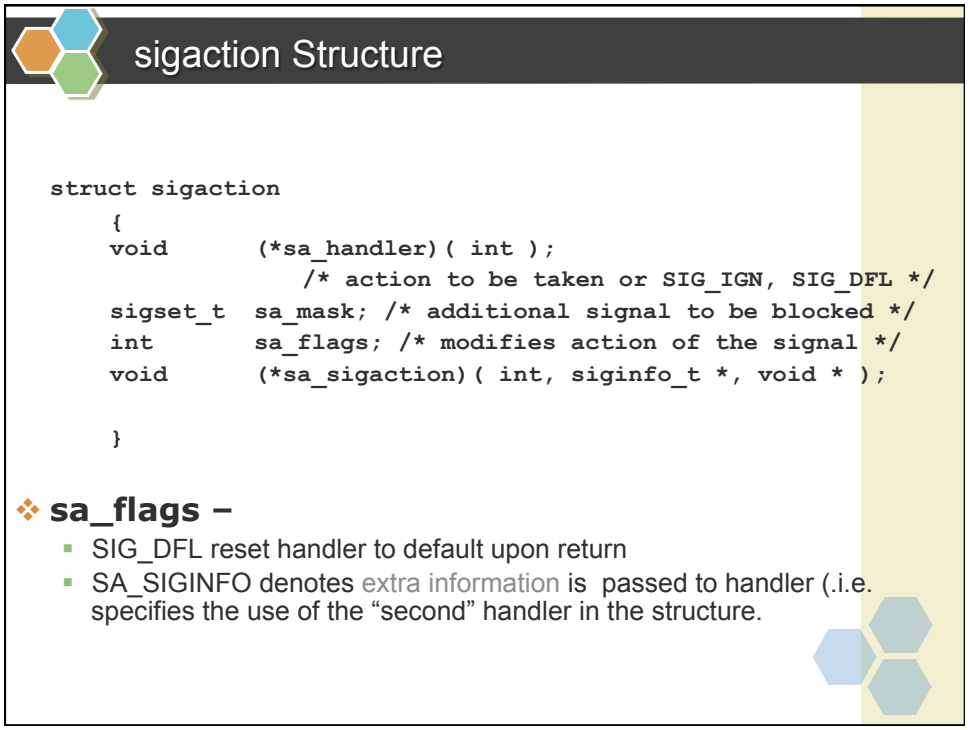
A Critical Code Region

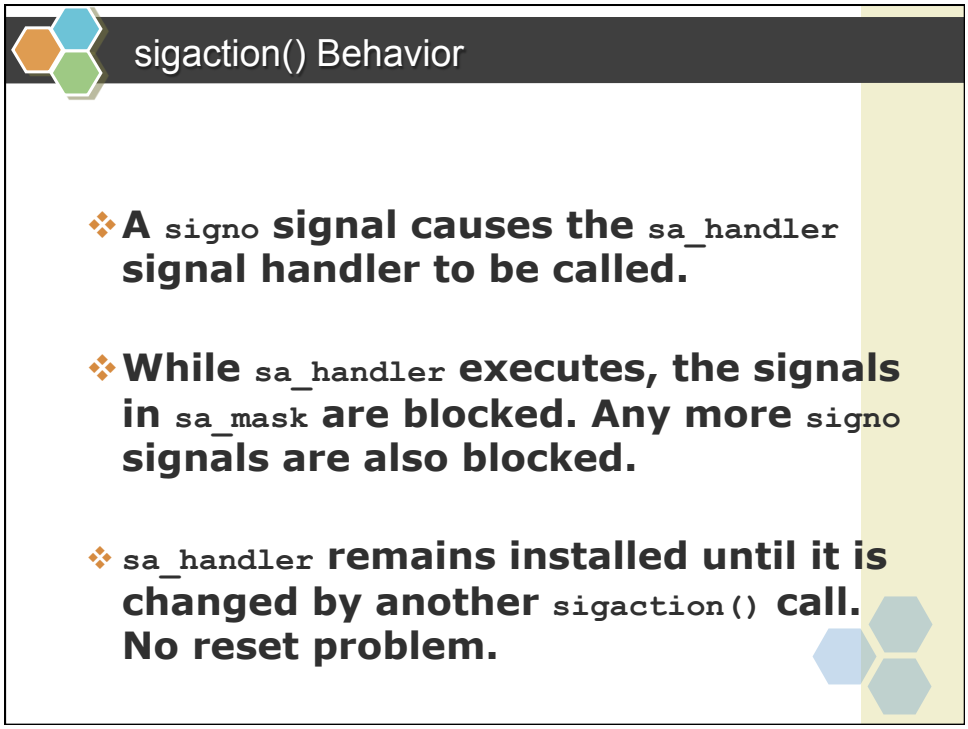
```
sigset_t newmask, oldmask;

sigemptyset( &newmask );
sigaddset( &newmask, SIGINT );

/* block SIGINT; save old mask */
sigprocmask( SIG_BLOCK, &newmask, &oldmask );

/* critical region of code */

/* reset mask which unblocks SIGINT */
sigprocmask( SIG_SETMASK, &oldmask, NULL );
```

7.3. sigaction()

- **Supercedes (more powerful than) `signal()`**
  - `sigaction()` can be used to code a non-resetting `signal()`

-
```
#include <signal.h>

int sigaction(int signo,
        const struct sigaction *act,
        struct sigaction *oldact );
```


sigaction Structure
struct sigaction
{
void (*sa_handler)(int);
/* action to be taken or SIG_IGN, SIG_DFL */
sigset_t sa_mask; /* additional signal to be blocked */
int sa_flags; /* modifies action of the signal */
void (*sa_sigaction)(int, siginfo_t *, void *);
}
sa_flags –
SIG_DFL reset handler to default upon return
SA_SIGINFO denotes extra information is passed to handler (.i.e. specifies the use of the "second" handler in the structure.


sigaction() Behavior
A signo signal causes the sa_handler signal handler to be called.
While sa_handler executes, the signals in sa_mask are blocked. Any more signo signals are also blocked.
sa_handler remains installed until it is changed by another sigaction() call. No reset problem.

Signal Raising

```
int main()
  {
  struct sigaction act;

  act.sa_handler = ouch;

  sigemptyset( &act.sa_mask );

  act.sa_flags = 0;

  SIGINT, &act, 0

  ("Hell
        sleep(1);
        }
  }
```

```
struct sigaction
    {
    void (*) (int) sa_handler
    sigset_t sa_mask
    int sa_flags
    }
```

Set the signal handler to be the function ouch

We can manipulate sets of signals..

No flags are needed here. Possible flags include: SA_NOCLDSTOP SA_RESETHAND

This call sets the signal handler for the SIGINT (ctrl-C) signal

Signal Raising

- This function will continually capture the ctrl-C (SIGINT) signal.
- Default behavior is not restored after signal is caught.
- To terminate the program, must type ctrl-\, the SIGQUIT signal.

sigexPOS.c

```
/* sigexPOS.c - demonstrate sigaction() */
/* include files as before */

int main(void)
{
   /* struct to deal with action on signal set */
   static struct sigaction act;

   void catchint(int); /* user signal handler */

   /* set up action to take on receipt of SIGINT */
   act.sa_handler = catchint;
```

```
    /* create full set of signals */
    sigfillset(&(act.sa_mask));

    /* before sigaction call, SIGINT will terminate
    * process */

    /* now, SIGINT will cause catchint to be executed */
    sigaction( SIGINT, &act, NULL );
    sigaction( SIGQUIT, &act, NULL );

    printf("sleep call #1\n");
    sleep(1);

    /* rest of program as before */
```

Signals - Ignoring signals

- **Other than SIGKILL and SIGSTOP, signals can be ignored:**
- **Instead of in the previous program:**

```
  act.sa_handler = catchint /* or whatever */
We use:
  act.sa_handler = SIG_IGN;
The ^C key  will be ignored
```

Restoring previous action

- **The third parameter to sigaction, oact, can be used:**

```
/* save old action */
sigaction( SIGTERM, NULL, &oact );

/* set new action */
act.sa_handler = SIG_IGN;

sigaction( SIGTERM, &act, NULL );

/* restore old action */
sigaction( SIGTERM, &oact, NULL );
```

A Basic signal()

```
#include <signal.h>

Sigfunc *signal( int signo, Sigfunc *func )
     {
     struct sigaction act, oact;

     act.sa_handler = func;
     sigemptyset( &act.sa_mask );
     act.sa_flags = 0;

     act.sa_flags |= SA_INTERRUPT;
     if( signo != SIGALRM )
            act.sa_flags |= SA_RESTART;
            /* any system call interrupted by a signal
      * other than alarm is restarted */
     if( sigaction( signo, &act, &oact) < 0 )
            return(SIG_ERR);
     return( oact.sa_handler );
     }
```

7.4. Other POSIX Functions

- `sigpending()` — **examine blocked signals**
- `sigsetjmp()` `siglongjmp()` — **jump functions for use in signal handlers which handle masks correctly**
- `sigsuspend()` — **atomically reset mask and sleep**

[sig]longjmp & [sig]setjmp

NOTES (longjmp, sigjmp)

POSIX does not specify whether longjmp will restore the signal context. If you want to save and restore signal masks, use siglongjmp.

NOTES (setjmp, sigjmp)

POSIX does not specify whether setjmp will save the signal context. (In SYSV it will not. In BSD4.3 it will, and there is a function _setjmp that will not.) If you want to save signal masks, use sigsetjmp.

Example

```
#include <stdio.h>
#include <signal.h>
#include <setjmp.h>

sigjmp_buf buf;

void handler(int sig)
    {
    siglongjmp(buf, 1);
    }

main()
{
  signal(SIGINT, handler);

  if( sigsetjmp(buf, 1) == 0 )
       printf("starting\n");
  else
       printf("restarting\n");
  …
```

```
  …
  while(1)
    {
        sleep(5);
        printf("  waiting...\n");
    }
}
```

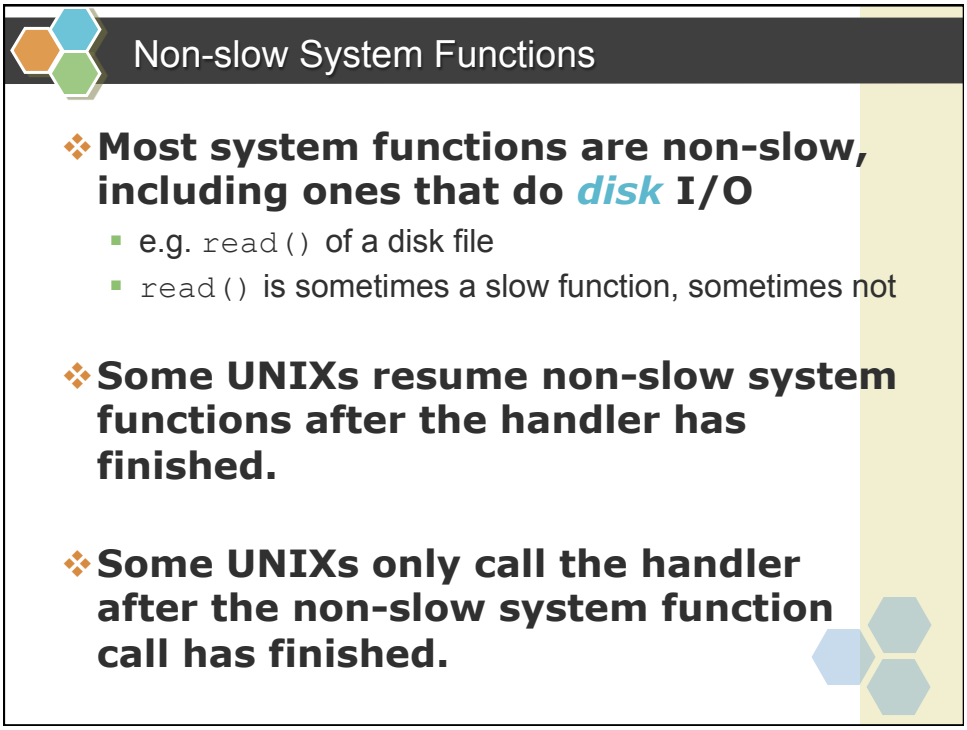
```
> a.out
starting
  waiting...
  waiting...        <-- Control-c
restarting
  waiting...
  waiting...
  waiting...
restarting          <-- Control-c
  waiting...
restarting          <-- Control-c
  waiting...
  waiting...
```

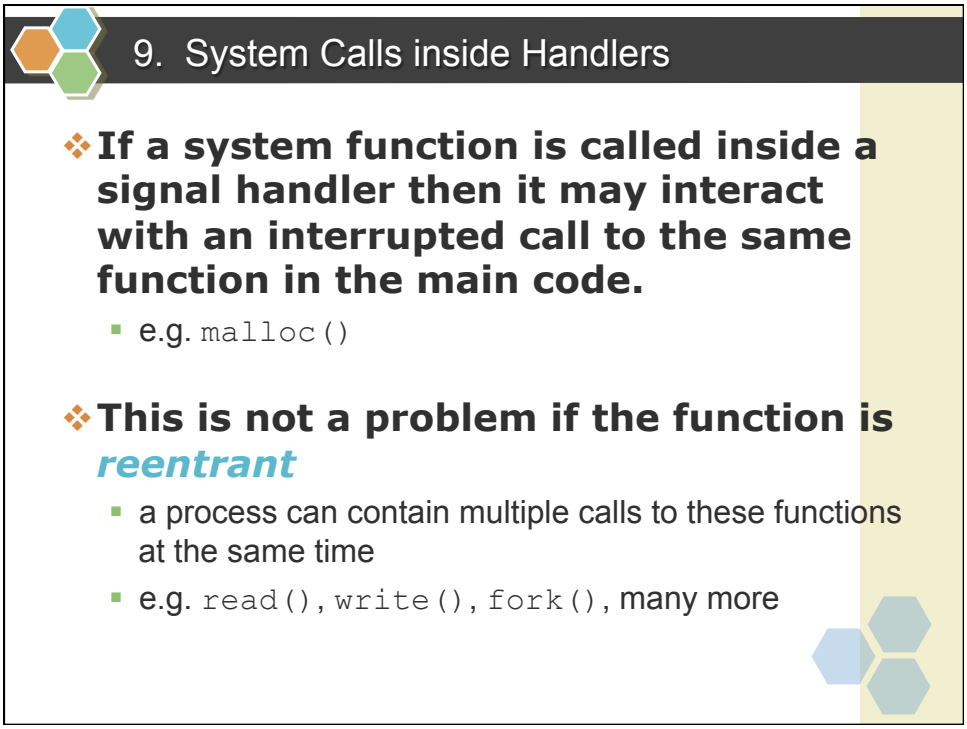
8. Interrupted System Calls

- **When a system call (e.g. `read()`) is interrupted by a signal, a signal handler is called, returns, and then what?**
- **On many UNIXs, *slow* system function calls do not resume. Instead they return an error and `errno` is assigned `EINTR`.**
  - true of Linux, but can be altered with (Linux-specific) `siginterrupt()`

Slow System Functions

- **Slow system functions carry out I/O on things that can possibly block the caller forever:**
  - pipes, terminal drivers, networks
  - some IPC functions
  - `pause()`, some uses of `ioctl()`
- **Can use signals on slow system functions to code up timeouts (e.g. did earlier)**


Non-slow System Functions
Most system functions are non-slow, including ones that do disk I/O
e.g. read() of a disk file
read() is sometimes a slow function, sometimes not
Some UNIXs resume non-slow system functions after the handler has finished.
Some UNIXs only call the handler after the non-slow system function call has finished.


9. System Calls inside Handlers
If a system function is called inside a signal handler then it may interact with an interrupted call to the same function in the main code.
e.g. malloc()
This is not a problem if the function is reentrant
a process can contain multiple calls to these functions at the same time
e.g. read(), write(), fork(), many more

Non-reentrant Functions

- **A functions may be non-reentrant (only one call to it at once) for a number of reasons:**
  - it uses a static data structure
  - it manipulates the heap: `malloc()`, `free()`, etc.
  - it uses the standard I/O library
    - e,g, `scanf()`, `printf()`
    - the library uses global data structures in a non-reentrant way

errno Problem

- **`errno` is usually represented by a global variable.**
- **Its value in the program can be changed suddenly by a signal handler which produces a new system function error.**