CS631 - Advanced Programming in the UNIX Environment

Department of Computer Science
Stevens Institute of Technology
Jan Schaumann
jschauma@stevens.edu
http://www.cs.stevens.edu/~jschauma/631/

In a nutshell: the ”what”

```
$ ls /bin
[          csh        ed         ls         pwd        sleep
cat        date       expr       mkdir      rcmd       stty
chio       dd         hostname   mt         rcp        sync
chmod      df         kill       mv         rm         systrace
cp         domainname ksh        pax        rmdir      tar
cpio       echo       ln         ps         sh         test
$
```

See also:

```
$ ssh linux-lab.cs.stevens.edu
$ cd ~jschauma/apue/src/
```

In a nutshell: the ”what”

```
$ grep "(int" /usr/include/sys/socket.h
int accept(int, struct sockaddr * __restrict, socklen_t * __restrict);
int bind(int, const struct sockaddr *, socklen_t);
int connect(int, const struct sockaddr *, socklen_t);
int getsockopt(int, int, int, void * __restrict, socklen_t * __restrict);
int listen(int, int);
ssize_t recv(int, void *, size_t, int);
ssize_t recvfrom(int, void * __restrict, size_t, int,
ssize_t recvmsg(int, struct msghdr *, int);
ssize_t send(int, const void *, size_t, int);
ssize_t sendto(int, const void *,
ssize_t sendmsg(int, const struct msghdr *, int);
int setsockopt(int, int, int, const void *, socklen_t);
int socket(int, int, int);
int socketpair(int, int, int, int *);
$
```

In a nutshell: the ”what”

- gain an understanding of the UNIX operating systems
- gain (systems) programming experience
- understand fundamental OS concepts (with focus on UNIX family):
  - multi-user concepts
  - basic and advanced I/O
  - process relationships
  - interprocess communication
  - basic network programming using a client/server model

In a nutshell: the ”how”

```
static char dot[] = ".", *dotav[] = { dot, NULL };
struct winsize win;
int ch, fts_options;
int kflag = 0;
const char *p;

setprogname(argv[0]);
setlocale(LC_ALL, "");

/* Terminal defaults to -Cq, non-terminal defaults to -1. */
if (isatty(STDOUT_FILENO)) {
    if (ioctl(STDOUT_FILENO, TIOCGWINSZ, &win) == 0 &&
        win.ws_col > 0)
        termwidth = win.ws_col;
    f_column = f_nonprint = 1;
} else
    f_singlecol = 1;

/* Root is -A automatically. */
if (!getuid())
    f_listdot = 1;

fts_options = FTS_PHYSICAL;
while ((ch = getopt(argc, argv, "1ABCFLRSTWabcdfghiklmnopqrstuwx")) != -1) {
    switch (ch) {
    /*
     * The -1, -C, -l, -m and -x options all override each other so
     * shell aliasing works correctly.
     */
    case '1':
        f_singlecol = 1;
```

In a nutshell: the ”how”

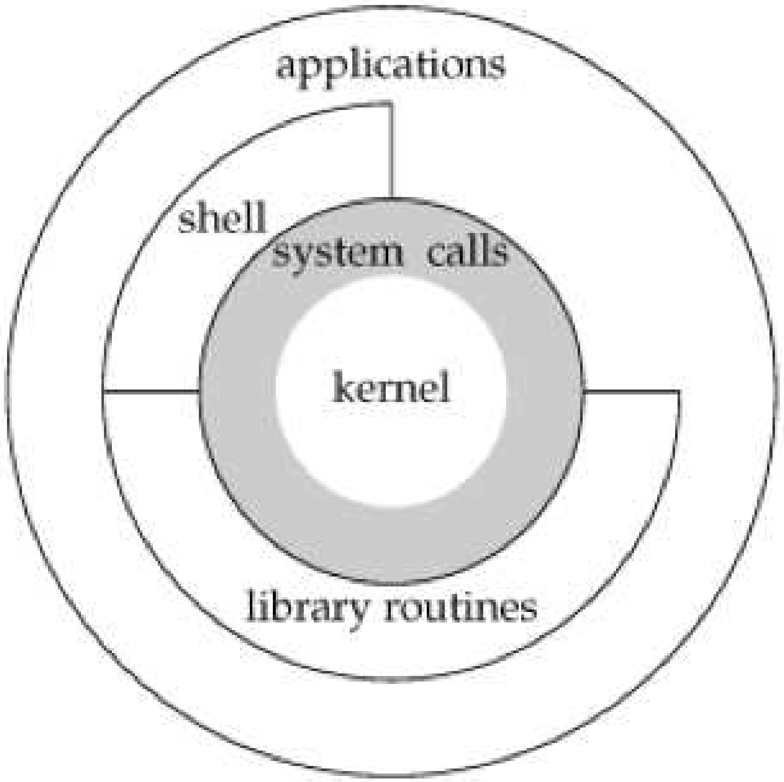
```
$ $EDITOR cmd.c
$ cc -Wall -g -o cmd cmd.c
cmd.c: In function ‘main’:
cmd.c:19: error: parse error before "return"
$ $EDITOR cmd.c
$ cc -Wall -g -o cmd cmd.c
$ ./cmd
Memory fault (core dumped)
$ echo "!@#!@!!!??#@!"
!@#!@!!!??#@!
$ gdb ./cmd cmd.core
Program terminated with signal 11, Segmentation fault.
Loaded symbols for /usr/libexec/ld.elf_so
#0  0xbbbc676a in __findenv () from /usr/lib/libc.so.12
(gdb)
```

In a nutshell

The ”why”:

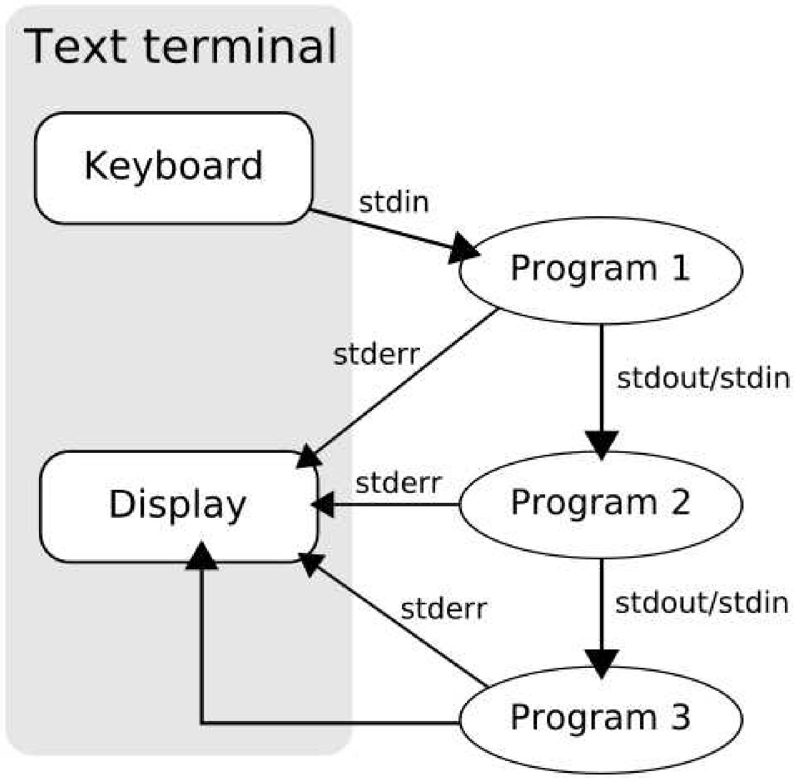
- understanding how UNIX works gives you insights in other OS concepts
- system level programming experience is invaluable as it forms the basis for most other programming and even *use* of the system
- system level programming in C helps you understand general programming concepts
- most higher level programming languages (eventually) call (or implement themselves) standard C library functions

UNIX Basics: Architecture



UNIX Basics: Pipelines

Say "Thank you, Douglas McIlroy!"



http://is.gd/vGHO9J

Program Design

”Consistency underlies all principles of quality.”
Frederick P. Brooks, Jr

Program Design

`https://en.wikipedia.org/wiki/Unix_philosophy`

UNIX programs...

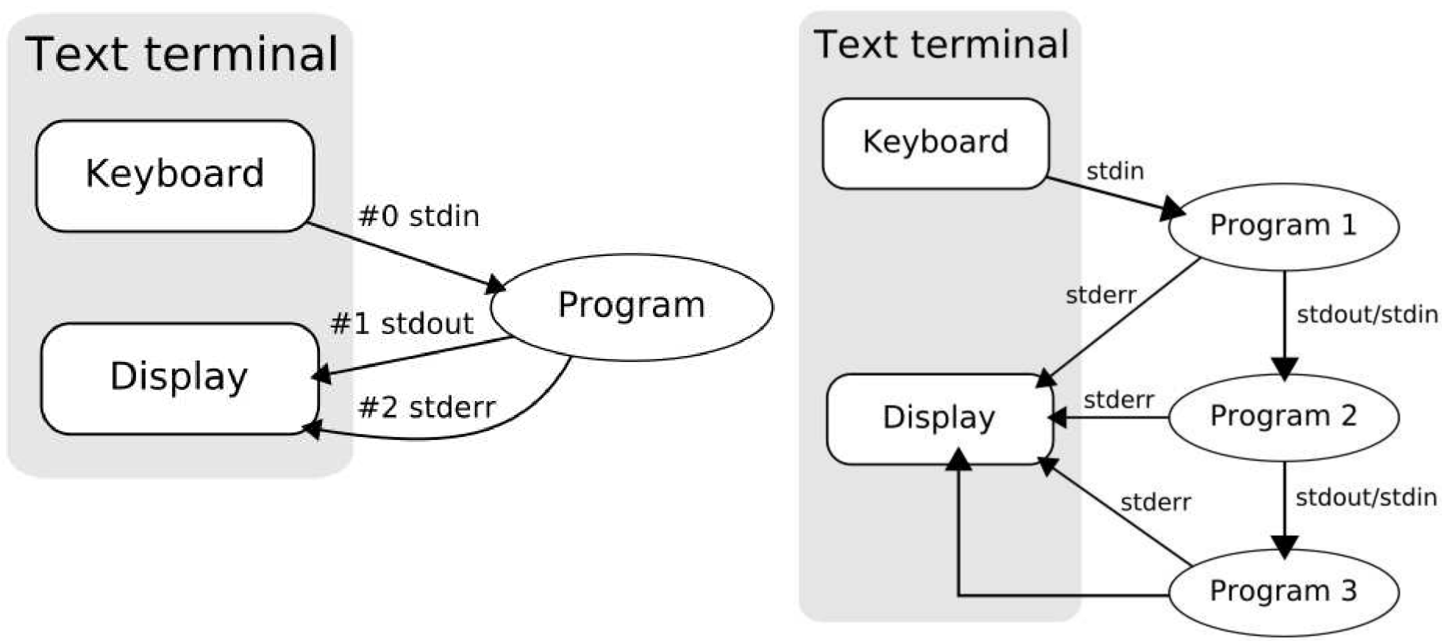
- ...are simple
- ...follow the element of least surprise
- ...accept input from `stdin`
- ...generate output to `stdout`
- ...generate meaningful error messages to `stderr`
- ...have meaningful exit codes
- ...have a manual page

Lecture 02

File I/O, File Sharing

File Descriptors

- A *file descriptor* (or *file handle*) is a small, non-negative integer which identifies a file to the kernel.
- Traditionally, `stdin`, `stdout` and `stderr` are 0, 1 and 2 respectively.



See also: `https://en.wikipedia.org/wiki/File_descriptor`

Standard I/O

Basic File I/O: almost all UNIX file I/O can be performed using these five functions:

- `open(2)`
- `close(2)`
- `lseek(2)`
- `read(2)`
- `write(2)`

Processes may want to share recources. This requires us to look at:

- atomicity of these operations
- file sharing
- manipulation of file descriptors

open(2)

```
#include <fcntl.h>

int open(const char *pathname, int oflag, ...  /* mode_t mode */ );
```

Returns: file descriptor if OK, -1 on error

oflag must be one (and only one) of:

- O_RDONLY – Open for reading only
- O_WRONLY – Open for writing only
- O_RDWR – Open for reading and writing

and may be OR'd with any of these:

- O_APPEND – Append to end of file for each write
- O_CREAT – Create the file if it doesn't exist. Requires *mode* argument
- O_EXCL – Generate error if O_CREAT and file already exists. (atomic)
- O_TRUNC – If file exists and successfully open in O_WRONLY or O_RDWR, make length = 0
- O_NOCTTY – If pathname refers to a terminal device, do not allocate the device as a controlling terminal
- O_NONBLOCK – If pathname refers to a FIFO, block special, or char special, set nonblocking mode (open and I/O)
- O_SYNC – Each write waits for physical I/O to complete

close(2)

```
#include <unistd.h>

int close(int fd);
```

Returns: 0 if OK, -1 on error

- closing a filedescriptor releases any record locks on that file (more on that in future lectures)
- file descriptors not explicitly closed are closed by the kernel when the process terminates.
- to avoid leaking file descriptors, always `close(2)` them within the same scope

read(2)

```
#include <unistd.h>

ssize_t read(int filedes, void *buff, size_t nbytes );
```

Returns: number of bytes read, 0 if end of file, -1 on error

There can be several cases where `read` returns less than the number of bytes requested:

- EOF reached before requested number of bytes have been read
- Reading from a terminal device, one ”line” read at a time
- Reading from a network, buffering can cause delays in arrival of data
- Record-oriented devices (magtape) may return data one record at a time
- Interruption by a signal

`read` begins reading at the current offset, and increments the offset by the number of bytes actually read.

write(2)

```
#include <unistd.h>

ssize_t write(int filedes, void *buff, size_t nbytes );
```

Returns: number of bytes written if OK, -1 on error

- `write` returns `nbytes` or an error has occurred
- for regular files, `write` begins writing at the current offset (unless `O_APPEND` has been specified, in which case the offset is first set to the end of the file)
- after the write, the offset is adjusted by the number of bytes actually written

lseek(2)

```
#include <sys/types.h>
#include <fcntl.h>

off_t lseek(int filedes, off_t offset, int whence );
```

Returns: new file offset if OK, -1 on error

The value of whence determines how offset is used:

- SEEK_SET bytes from the beginning of the file
- SEEK_CUR bytes from the current file position
- SEEK_END bytes from the end of the file

“Weird” things you can do using `lseek(2)`:

- seek to a negative offset
- seek 0 bytes from the current position
- seek past the end of the file

lseek(2)

```
$ cc -Wall hole.c
$ ./a.out
$ ls -l file.hole
-rw-------  1 jschauma  wheel  10240020 Sep 18 17:20 file.hole
$ hexdump -c file.hole
0000000   a   b   c   d   e   f   g   h   i   j  \0  \0  \0  \0  \0  \0
0000010  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0
*
09c4000  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0   A   B   C   D   E   F
09c4010   G   H   I   J
09c4014
$ cat file.hole > file.nohole
$ ls -ls file.*
   96 -rw-------  1 jschauma  wheel  10240020 Sep 18 17:20 file.hole
20064 -rw-r--r--  1 jschauma  wheel  10240020 Sep 18 17:21 file.nohole
```

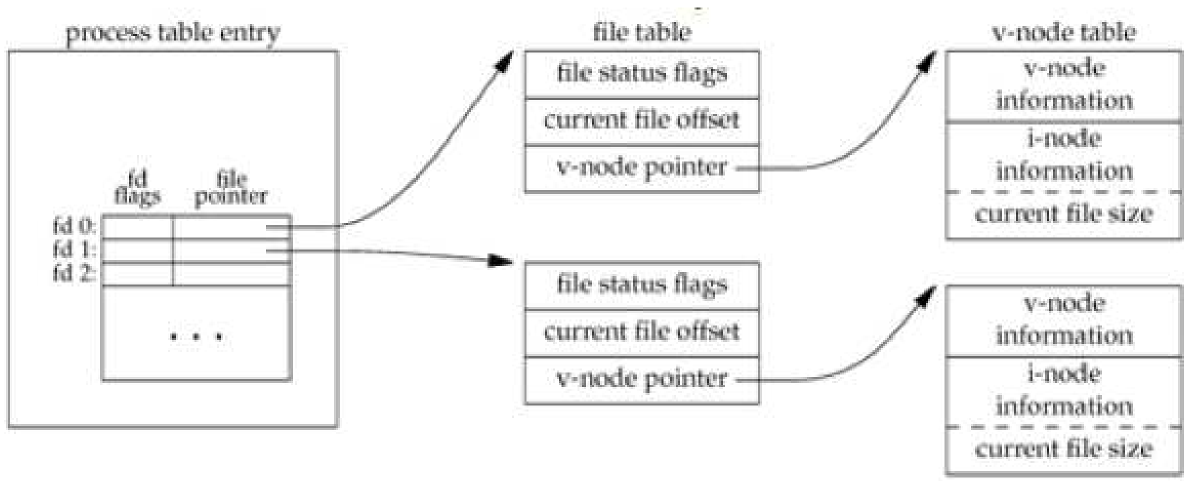
https://en.wikipedia.org/wiki/Sparse_file (not on HFS+ / NFS)

File Sharing

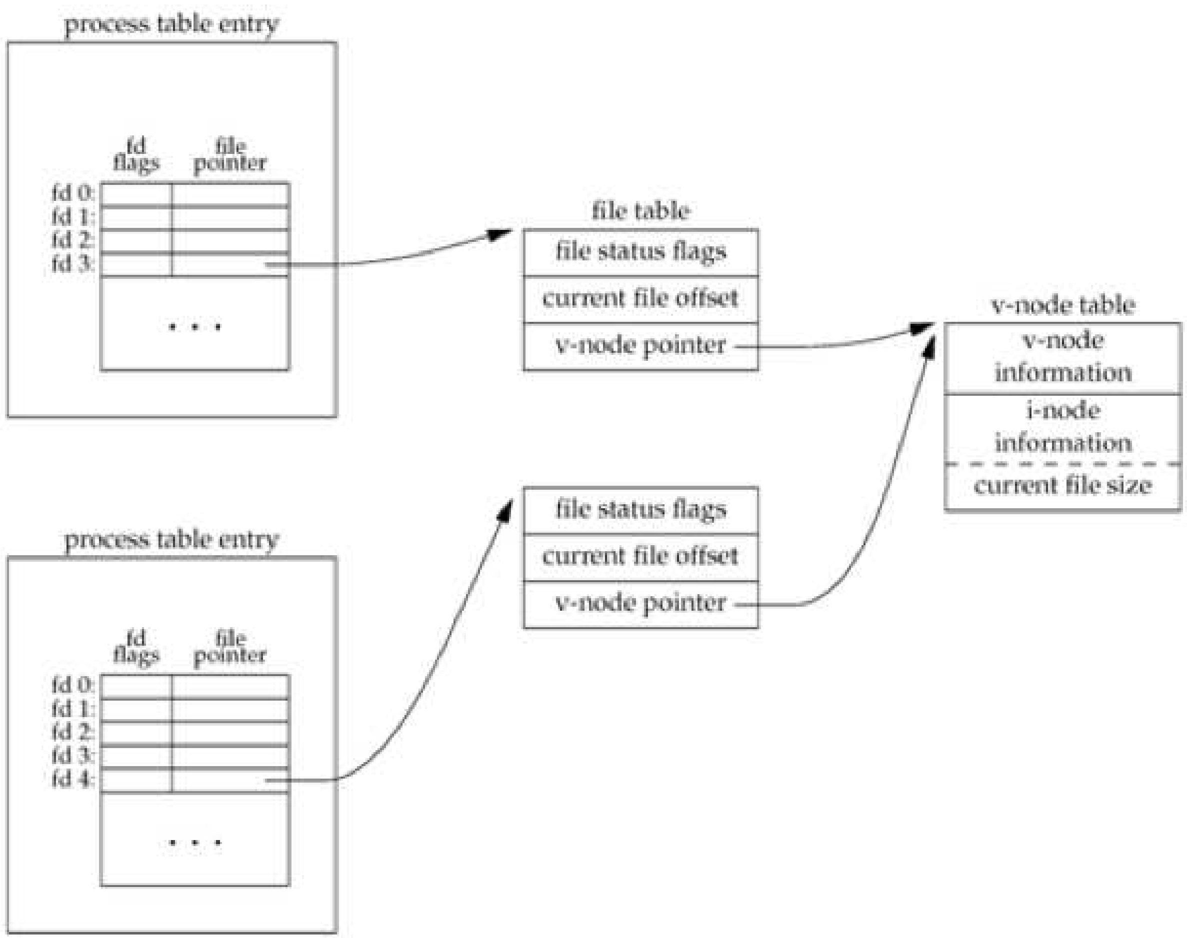
Since UNIX is a multi-user/multi-tasking system, it is conceivable (and useful) if more than one process can act on a single file simultaneously. In order to understand how this is accomplished, we need to examine some kernel data structures which relate to files. (See: Stevens, pp 75 ff)

- each process table entry has a table of file descriptors, which contain
  - the file descriptor flags (ie `FD_CLOEXEC`, see `fcntl(2)`)
  - a pointer to a file table entry
- the kernel maintains a file table; each entry contains
  - file status flags (`O_APPEND`, `O_SYNC`, `O_RDONLY`, etc.)
  - current offset
  - pointer to a vnode table entry
- a vnode structure contains
  - vnode information
  - inode information (such as current file size)

File Sharing



File Sharing



File Sharing

Knowing this, here's what happens with each of the calls we discussed earlier:

- after each `write` completes, the current file offset in the file table entry is incremented. (If current_file_offset $>$ current_file_size, change current file size in i-node table entry.)
- If file was opened `O_APPEND` set corresponding flag in file status flags in file table. For each `write`, current file offset is first set to current file size from the i-node entry.
- `lseek` simply adjusts current file offset in file table entry
- to `lseek` to the end of a file, just copy current file size into current file offset.

Atomic Operations

In order to ensure consistency across multiple writes, we require *atomicity* in some operations.

An operation is atomic if either *all* of the steps are performed or *none* of the steps are performed.

Suppose UNIX didn't have `O_APPEND` (early versions didn't). To append, you'd have to do this:

```
if (lseek(fd, 0L, 2) < 0) {        /* position to EOF */
    fprintf(stderr, "lseek error\n");
    exit(1);
}

if (write(fd, buff, 100) != 100) { /* ...and write */
    fprintf(stderr, "write error\n");
    exit(1);
}
```

What if another process was doing the same thing to the same file?

Lecture 03

Files and Directories

`stat(2)` family of functions

```
#include <sys/types.h>
#include <sys/stat.h>

int stat(const char *path, struct stat *sb);
int lstat(const char *path, struct stat *sb);
int fstat(int fd, struct stat *sb);
```

Returns: 0 if OK, -1 on error

All these functions return extended attributes about the referenced file (in the case of *symbolic links*, `lstat(2)` returns attributes of the *link*, others return stats of the referenced file).

```
struct stat {
    dev_t     st_dev;        /* device number (filesystem) */
    ino_t     st_ino;        /* i-node number (serial number) */
    mode_t    st_mode;       /* file type & mode (permissions) */
    dev_t     st_rdev;       /* device number for special files */
    nlink_t   st_nlink;      /* number of links */
    uid_t     st_uid;        /* user ID of owner */
    gid_t     st_gid;        /* group ID of owner */
    off_t     st_size;       /* size in bytes, for regular files */
    time_t    st_atime;      /* time of last access */
    time_t    st_mtime;      /* time of last modification */
    time_t    st_ctime;      /* time of last file status change */
    long      st_blocks;     /* number of 512-byte* blocks allocated */
    long      st_blksize;    /* best I/O block size */
};
```

`struct stat`: `st_mode`

The `st_mode` field of the `struct stat` encodes the type of file:

- **regular** – most common, interpretation of data is up to application
- **directory** – contains names of other files and pointer to information on those files. Any process can read, only kernel can write.
- **character special** – used for certain types of devices
- **block special** – used for disk devices (typically). All devices are either *character* or *block special*.
- **FIFO** – used for interprocess communication (sometimes called *named pipe*)
- **socket** – used for network communication and non-network communication (same host).
- **symbolic link** – Points to another file.

Find out more in `<sys/stat.h>`.

`struct stat`: `st_mode`, `st_uid` and `st_gid`

Every process has six or more IDs associated with it:

real user ID real group ID	who we really are
effective user ID effective group ID supplementary group IDs	used for file access permission checks
saved set-user-ID saved set-group-ID	saved by `exec` functions

Whenever a file is *setuid*, set the *effective user ID* to `st_uid`. Whenever a file is *setgid*, set the *effective group ID* to `st_gid`. `st_uid` and `st_gid` always specify the owner and group owner of a file, regardless of whether it is setuid/setgid.

struct stat: st_mode

st_mode also encodes the file access permissions (S_IRUSR, S_IWUSR, S_IXUSR, S_IRGRP, S_IWGRP, S_IXGRP, S_IROTH, S_IWOTH, S_IXOTH). Uses of the permissions are summarized as follows:

- To open a file, need execute permission on each directory component of the path
- To open a file with O_RDONLY or O_RDWR, need read permission
- To open a file with O_WRONLY or O_RDWR, need write permission
- To use O_TRUNC, must have write permission
- To create a new file, must have write+execute permission for the directory
- To delete a file, need write+execute on directory, file doesn't matter
- To execute a file (via exec family), need execute permission

struct stat: st_mode

Which permission set to use is determined (in order listed):

1. If effective-uid == 0, grant access
2. If effective-uid == `st_uid`
   2.1. if appropriate user permission bit is set, grant access
   2.2. else, deny access
3. If effective-gid == `st_gid`
   3.1. if appropriate group permission bit is set, grant access
   3.2. else, deny access
4. If appropriate other permission bit is set, grant access, else deny access

`struct stat`: `st_mode`

Ownership of **new** files and directories:

- `st_uid` = effective-uid
- `st_gid` = ...either:
  - effective-gid of process
  - gid of directory in which it is being created

umask(2)

```
#include <sys/stat.h>

mode_t umask(mode_t numask);
```

Returns: previous file mode creation mask

`umask(2)` sets the file creation mode mask. Any bits that are *on* in the file creation mask are turned *off* in the file's mode.

Important because a user can set a default umask. If a program needs to be able to insure certain permissions on a file, it may need to turn off (or modify) the umask, which affects only the current process.

chmod(2), lchmod(2) and fchmod(2)

```
#include <sys/stat.h>

int chmod(const char *path, mode_t mode);
int lchmod(const char *path, mode_t mode);
int fchmod(int fd, mode_t mode);
```

Returns: 0 if OK, -1 on error

Changes the permission bits on the file. Must be either superuser or *effective uid* == `st_uid`. *mode* can be any of the bits from our discussion of `st_mode` as well as:

- `S_ISUID` – setuid
- `S_ISGID` – setgid
- `S_ISVTX` – sticky bit (aka “saved text”)
- `S_IRWXU` – user read, write and execute
- `S_IRWXG` – group read, write and execute
- `S_IRWXO` – other read, write and execute

chown(2), lchown(2) and fchown(2)

```
#include <unistd.h>

int chown(const char *path, uid_t owner, gid_t group);
int lchown(const char *path, uid_t owner, gid_t group);
int fchown(int fd, uid_t owner, gid_t group);
```

Returns: 0 if OK, -1 on error

Changes `st_uid` and `st_gid` for a file. For BSD, must be superuser. Some SVR4's let users chown files they own. POSIX.1 allows either depending on `_POSIX_CHOWN_RESTRICTED` (a kernel constant).

owner or *group* can be -1 to indicate that it should remain the same. Non-superusers can change the `st_gid` field if both:

- effective-user ID == `st_uid` and
- *owner* == file's user ID and *group* == effective-group ID (or one of the supplementary group IDs)

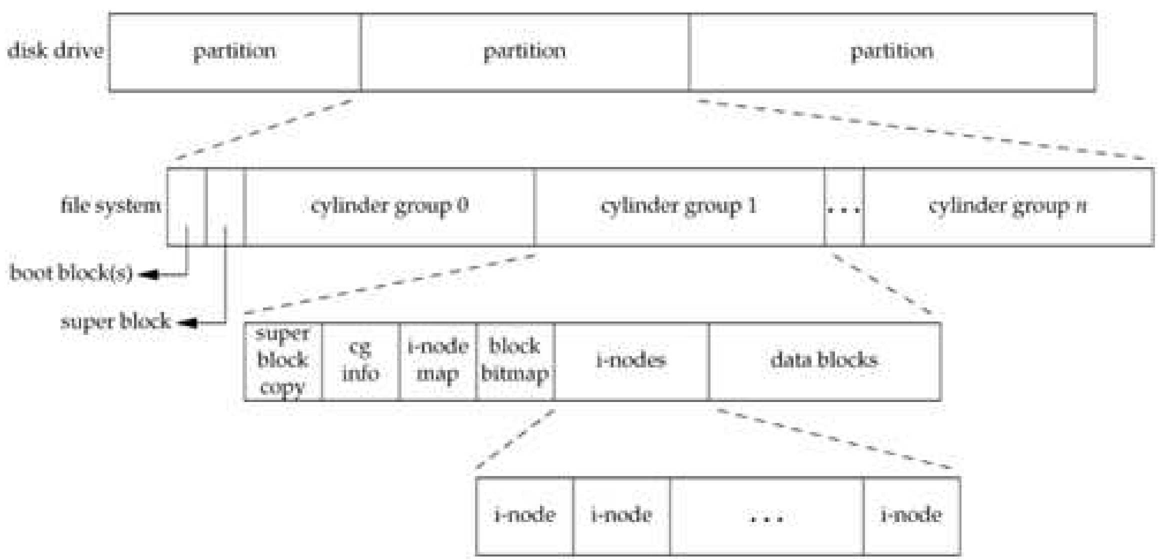
`chown` and friends clear all setuid or setgid bits.

Lecture 04

File Systems, System Data Files, Time & Date

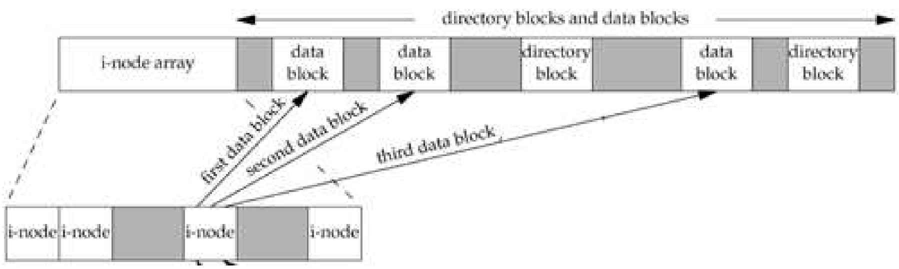
File Systems

- a disk can be divided into logical *partitions*
- each logical *partition* may be further divided into *file systems* containing *cylinder groups*
- each *cylinder group* contains a list of *inodes* (*i-list*) as well as the actual *directory*- and *data blocks*



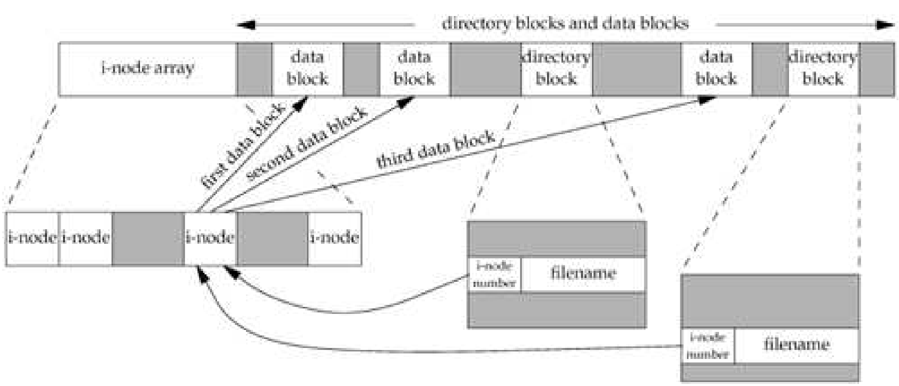
File Systems

- a disk can be divided into logical *partitions*
- each logical *partition* may be further divided into *file systems* containing *cylinder groups*
- each *cylinder group* contains a list of *inodes* (*i-list*) as well as the actual *directory*- and *data blocks*



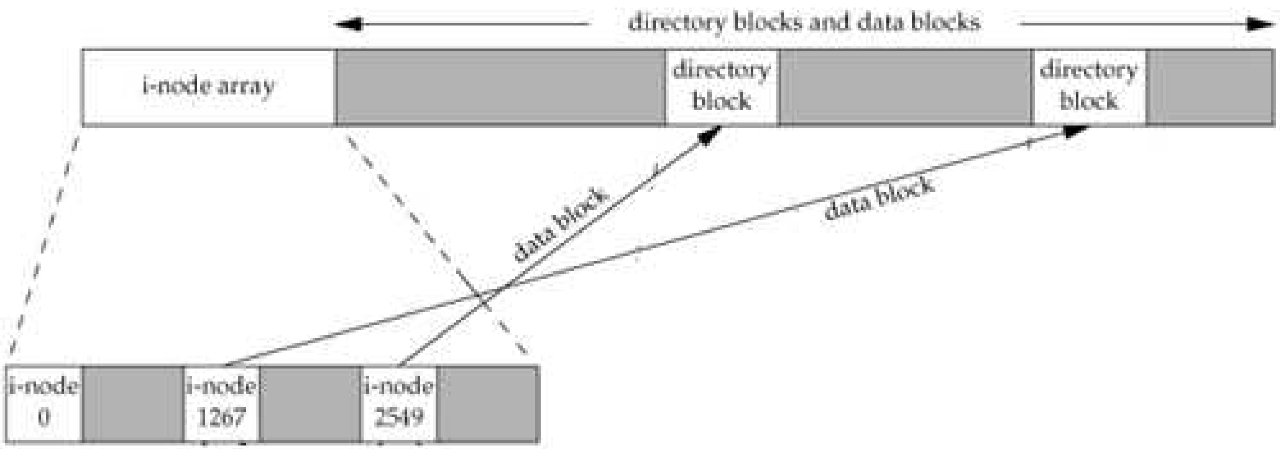
File Systems

- a disk can be divided into logical *partitions*
- each logical *partition* may be further divided into *file systems* containing *cylinder groups*
- each *cylinder group* contains a list of *inodes* (*i-list*) as well as the actual *directory-* and *data blocks*
- a directory entry is really just a *hard link* mapping a “filename” to an inode
- you can have many such mappings to the same file



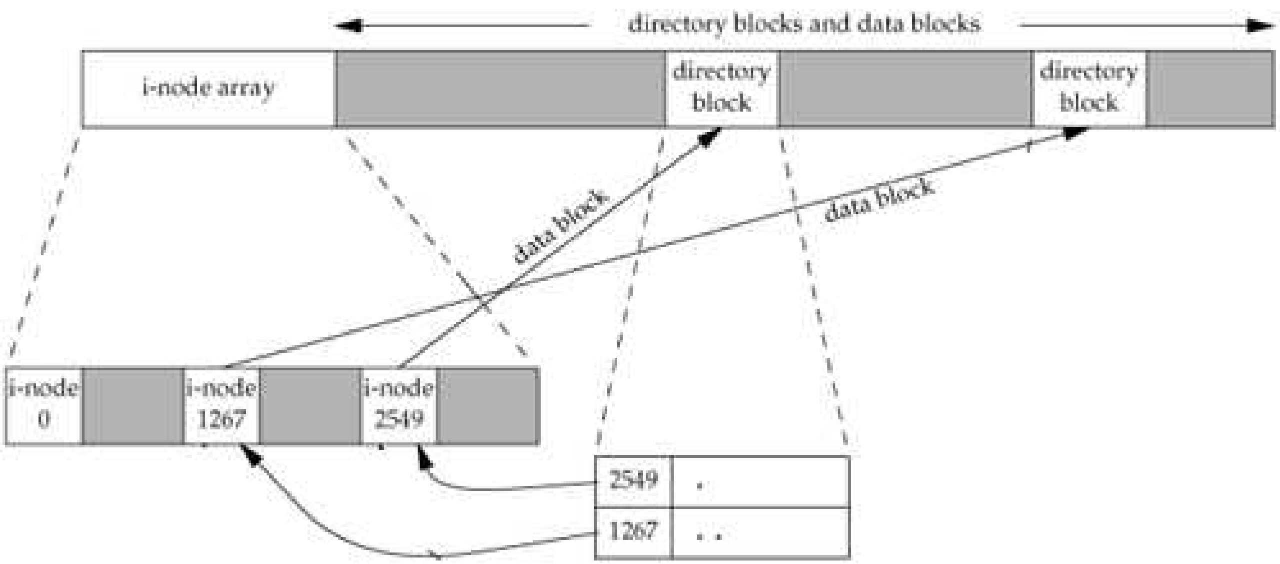
Directories

- directories are special ”files” containing hardlinks



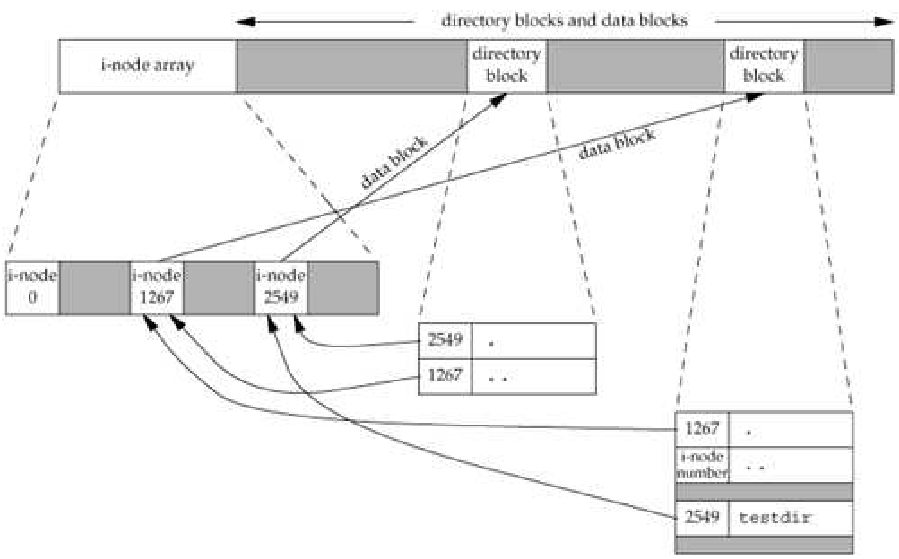
Directories

- directories are special ”files” containing hardlinks
- each directory contains at least two entries:
  - . (*this* directory)
  - . . (the parent directory)



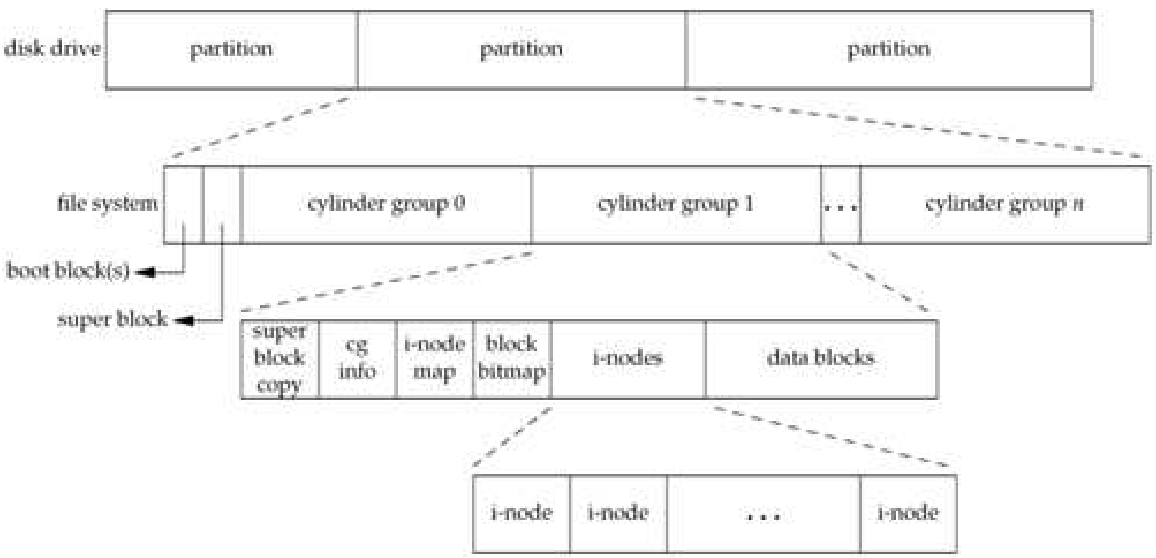
Directories

- directories are special "files" containing hardlinks
- each directory contains at least two entries:
  - . (*this* directory)
  - . . (the parent directory)
- the link count (`st_nlink`) of a directory is at least 2



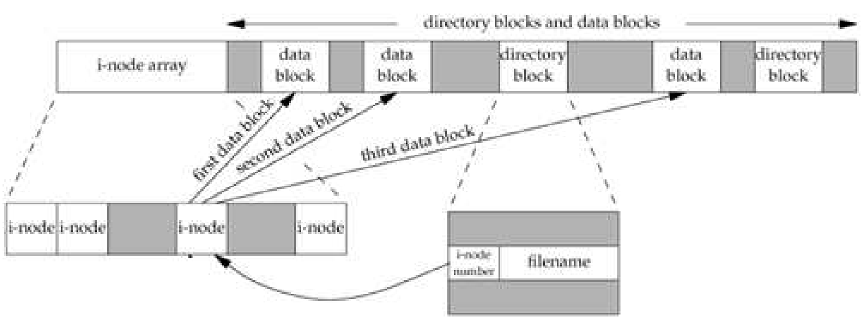
Inodes

- the *inode* contains most of information found in the `stat` structure.
- every *inode* has a *link count* (`st_nlink`): it shows how many "things" point to this inode. Only if this *link count* is 0 (and no process has the file open) are the *data blocks* freed.
- *inode* number in a directory entry must point to an *inode* on the same file system (no hardlinks across filesystems)



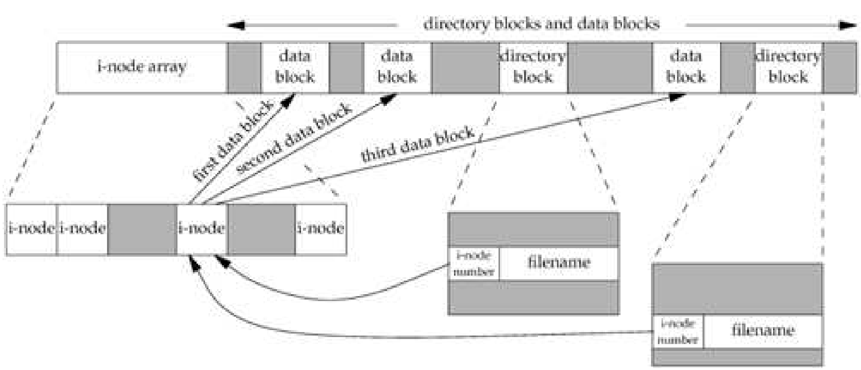
Inodes

- the *inode* contains most of information found in the `stat` structure.
- every *inode* has a *link count* (`st_nlink`): it shows how many “things” point to this inode. Only if this *link count* is 0 (and no process has the file open) are the *data blocks* freed.
- *inode* number in a directory entry must point to an *inode* on the same file system (no hardlinks across filesystems)
- to move a file within a single filesystem, we can just ”move” the directory entry (actually done by creating a new entry, and deleting the old one).



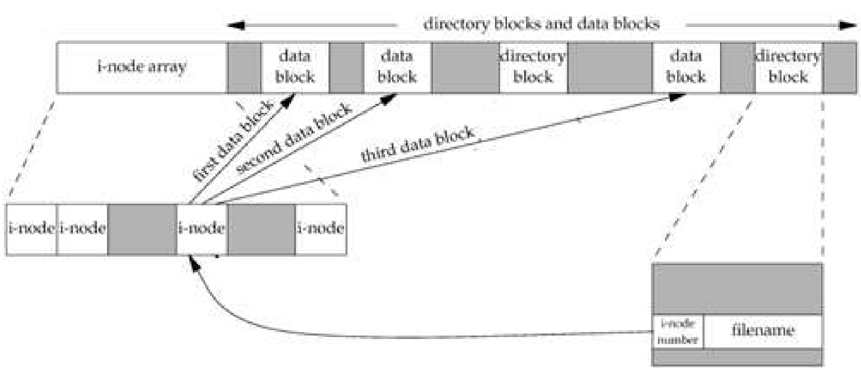
Inodes

- the *inode* contains most of information found in the `stat` structure.
- every *inode* has a *link count* (`st_nlink`): it shows how many “things” point to this inode. Only if this *link count* is 0 (and no process has the file open) are the *data blocks* freed.
- *inode* number in a directory entry must point to an *inode* on the same file system (no hardlinks across filesystems)
- to move a file within a single filesystem, we can just ”move” the directory entry (actually done by creating a new entry, and deleting the old one).



Inodes

- the *inode* contains most of information found in the `stat` structure.
- every *inode* has a *link count* (`st_nlink`): it shows how many “things” point to this inode. Only if this *link count* is 0 (and no process has the file open) are the *data blocks* freed.
- *inode* number in a directory entry must point to an *inode* on the same file system (no hardlinks across filesystems)
- to move a file within a single filesystem, we can just ”move” the directory entry (actually done by creating a new entry, and deleting the old one).



link(2) and unlink(2)

```
#include <unistd.h>

int link(const char *name1, const char *name2);
```

Returns: 0 if OK, -1 on error

- Creates a link to an existing file (hard link).
- POSIX.1 allows links to cross filesystems, most implementations (SVR4, BSD) don't.
- only uid(0) can create links to directories (loops in filesystem are bad)

```
#include <unistd.h>

int unlink(const char *path);
```

Returns: 0 if OK, -1 on error

- removes directory entry and decrements link count of file
- if file link count == 0, free data blocks associated with file (...unless processes have the file open)

rename(2)

```
#include <stdio.h>

int rename(const char *from, const char *to);
```

Returns: 0 if OK, -1 on error

If *oldname* refers to a file:

- if *newname* exists and it is not a directory, it's removed and *oldname* is renamed *newname*
- if *newname* exists and it is a directory, an error results
- must have w+x perms for the directories containing *old*/*newname*

If *oldname* refers to a directory:

- if *newname* exists and is an empty directory (contains only . and ..), it is removed; *oldname* is renamed *newname*
- if *newname* exists and is a file, an error results
- if *oldname* is a prefix of *newname* an error results
- must have w+x perms for the directories containing *old*/*newname*

Symbolic Links

```
#include <unistd.h>

int symlink(const char *name1, const char *name2);
```

Returns: 0 if OK, -1 on error

- file whose ”data” is a path to another file
- anyone can create symlinks to directories or files
- certain functions dereference the link, others operate on the link

```
#include <unistd.h>

int readlink(const char *path, char *buf, size_t bufsize);
```

Returns: number of bytes placed into buffer if OK, -1 on error

This function combines the actions of `open`, `read`, and `close`.
Note: *buf* is **not** NUL terminated.

File Times

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

int utimes(const char *path, const struct timeval times[2]);
int lutimes(const char *path, const struct timeval times[2]);
int futimes(int fd, const struct timeval times[2]);
```

Returns: 0 if OK, -1 on error

If *times* is NULL, access time and modification time are set to the current time (must be owner of file or have write permission). If *times* is non-NULL, then times are set according to the `timeval struct` array. For this, you must be the owner of the file (write permission not enough).

Note that `st_ctime` is set to the current time in both cases.

For the effect of various functions on the access, modification and changes-status times see Stevens, p. 117.

Note: some systems implement `lutimes(3)` (library call) via `utimes(2)` syscalls.

`mkdir(2)` and `rmdir(2)`

```
#include <sys/types.h>
#include <sys/stat.h>

int mkdir(const char *path, mode_t mode);
```

Returns: 0 if OK, -1 on error

Creates a new, empty (except for . and .. entries) directory. Access permissions specified by *mode* and restricted by the `umask(2)` of the calling process.

```
#include <unistd.h>

int rmdir(const char *path);
```

Returns: 0 if OK, -1 on error

If the link count is 0 (after this call), and no other process has the directory open, directory is removed. Directory must be empty (only . and .. remaining)

Reading Directories

```
#include <sys/types.h>
#include <dirent.h>

DIR *opendir(const char *filename);
                                    Returns: pointer if OK, NULL on error

struct dirent *readdir(DIR *dp);
                      Returns: pointer if OK, NULL at end of dir or on error

void rewinddir(DIR *dp);
int closedir(DIR *dp);
                                            Returns: 0 if OK, -1 on error
```

- read by anyone with read permission on the directory
- format of directory is implementation dependent (always use readdir and friends)

`opendir`, `readdir` and `closedir` should be familiar from our small `ls` clone. `rewinddir` resets an open directory to the beginning so readdir will again return the first entry.

For directory traversal, consider `fts(3)` (not available on all UNIX versions).

Moving around directories

```
#include <unistd.h>

char *getcwd(char *buf, size_t size);
```

Returns: *buf* if OK, `NULL` on error

Get the kernel's idea of our process's current working directory.

```
#include <unistd.h>

int chdir(const char *path);
int fchdir(int fd);
```

Returns: 0 if OK, -1 on error

Allows a process to change its current working directory. Note that `chdir` and `fchdir` affect only the current process.

```
$ cc -Wall cd.c
$ ./a.out /tmp
```

Password File

```
#include <sys/types.h>
#include <pwd.h>

struct passwd *getpwuid(uid_t uid);
struct passwd *getpwnam(const char *name);
```

Returns: pointer if OK, NULL on error

```
#include <sys/types.h>
#include <pwd.h>

struct passwd *getpwent(void);
```

Returns: pointer if OK, NULL on error

```
void setpwent(void);
void endpwent(void);
```

- `getpwent` returns next password entry in file each time it's called, no order
- `setpwent` rewinds to ”beginning” of entries
- `endpwent` closes the file(s)

See also: `getspnam(3)/getspent(3)` (where available)

Group File

```
#include <sys/types.h>
#include <grp.h>

struct group *getgrgid(gid_t gid);
struct group *getgrnam(const char *name);
```

Returns: pointer if OK, NULL on error

These allow us to look up an entry given a user's group name or numerical GID. What if we need to go through the group file entry by entry? Nothing in POSIX.1, but SVR4 and BSD give us:

```
#include <sys/types.h>
#include <grp.h>

struct group *getgrent(void);
```

Returns: pointer if OK, NULL on error

```
void setgrent(void);
void endgrent(void);
```

- `getgrent` returns next group entry in file each time it's called, no order
- `setgrent` rewinds to ”beginning” of entries
- `endgrent` closes the file(s)

Time and Date

```
#include <time.h>

time_t time(time_t *tloc);
                         Returns: value of time if OK, -1 on error
```

- Time is kept in UTC
- Time conversions (timezone, daylight savings time) handled "automatically"
- Time and date kept in a single quantity (`time_t`)

We can break this `time_t` value into its components with either of the following:

```
#include <time.h>

struct tm *gmtime(const time_t *calptr);
struct tm *localtime(const time_t *calptr);
                         Returns: pointer to broken down time
```

Time and Date

```
#include <time.h>

time_t mktime(struct tm *tmptr);
                         Returns: calendar time if OK, -1 on error
```

`localtime(3)` takes into account daylight savings time and the *TZ* environment variable. The `mktime(3)` function operates in the reverse direction. To output human readable results, use:

```
#include <time.h>

char *asctime(const struct tm *tmptr);
char *ctime(const struct tm *tmptr);
                         Returns: pointer to NULL terminated string
```

Lastly, there is a `printf(3)` like function for times:

```
#include <time.h>

size_t strftime(char *buf, size_t maxsize, const char *restricted format, const struct tm *timeptr);
                         Returns: number of characters stored in array if room, else 0
```

Lecture 05

Process Environment, Process Control

The `main` function

```
int main(int argc, char **argv);
```

- C program started by kernel (by one of the `exec` functions)
- special startup routine called by kernel which sets up things for `main` (or whatever entrypoint is defined)
- `argc` is a count of the number of command line arguments (including the command itself)
- `argv` is an array of pointers to the arguments
- it is guaranteed by both ANSI C and POSIX.1 that `argv[argc] == NULL`

Process Creation

On Linux:

```
$ cc -Wall entry.c
$ readelf -h a.out | more
ELF Header:
[...]
  Entry point address:               0x400460
  Start of program headers:          64 (bytes into file)
  Start of section headers:          4432 (bytes into file)
$ objdump -d a.out
[...]
0000000000400460 <_start>:
  400460:       31 ed                   xor    %ebp,%ebp
  400462:       49 89 d1                mov    %rdx,%r9
[...]
$
```

Process Creation

glibc/sysdeps/x86_64/start.S

```
0000000000401058 <_start>:
  401058:       31 ed                   xor    %ebp,%ebp
  40105a:       49 89 d1                mov    %rdx,%r9
  40105d:       5e                      pop    %rsi
  40105e:       48 89 e2                mov    %rsp,%rdx
  401061:       48 83 e4 f0             and    $0xfffffffffffffff0,%rsp
  401065:       50                      push   %rax
  401066:       54                      push   %rsp
  401067:       49 c7 c0 e0 1a 40 00    mov    $0x401ae0,%r8
  40106e:       48 c7 c1 50 1a 40 00    mov    $0x401a50,%rcx
  401075:       48 c7 c7 91 11 40 00    mov    $0x401191,%rdi
  40107c:       e8 2f 01 00 00          callq  4011b0 <__libc_start_main>
  401081:       f4                      hlt
  401082:       90                      nop
  401083:       90                      nop
```

Process Creation

glibc/csu/lic-start.c

```
STATIC int
LIBC_START_MAIN (int (*main) (int, char **, char ** MAIN_AUXVEC_DECL),
                 int argc, char **argv,
                 __typeof (main) init,
                 void (*fini) (void),
                 void (*rtld_fini) (void), void *stack_end)
{
[...]
  result = main (argc, argv, __environ MAIN_AUXVEC_PARAM);

  exit (result);
}
```

Process Creation

On Linux:

```
$ cc -Wall entry.c
$ readelf -h a.out | more
ELF Header:
[...]
  Entry point address:                 0x400460
  Start of program headers:            64 (bytes into file)
  Start of section headers:            4432 (bytes into file)
$ objdump -d a.out
[...]
0000000000400460 <_start>:
  400460:       31 ed                     xor    %ebp,%ebp
  400462:       49 89 d1                  mov    %rdx,%r9
[...]
$
```

Process Creation

On Linux:

```
$ cc -e foo entry.c
$ ./a.out
Foo for the win!
Memory fault
$ cc -e bar entry.c
$ ./a.out
bar rules!
$ echo $?
1
$ cc entry.c
$ ./a.out
Hooray main!
$ echo $?
13
$
```

Process Termination

There are 8 ways for a process to terminate.

Normal termination:

- return from `main`
- calling `exit`
- calling `_exit` (or `_Exit`)
- return of last thread from its start routine
- calling `pthread_exit` from last thread

Process Termination

There are 8 ways for a process to terminate.

Normal termination:

- return from `main`
- calling `exit`
- calling `_exit` (or `_Exit`)
- return of last thread from its start routine
- calling `pthread_exit` from last thread

Abnormal termination:

- calling `abort`
- terminated by a signal
- response of the last thread to a cancellation request

exit(3) and _exit(2)

```
#include <stdlib.h>
void exit(int status);
void _Exit(int status);

#include <unistd.h>
void _exit(int status);
```

- `_exit` and `_Exit`
  - return to the kernel immediately
  - `_exit` required by POSIX.1
  - `_Exit` required by ISO C99
  - synonymous on Unix
- `exit` does some cleanup and then returns
- both take integer argument, aka *exit status*

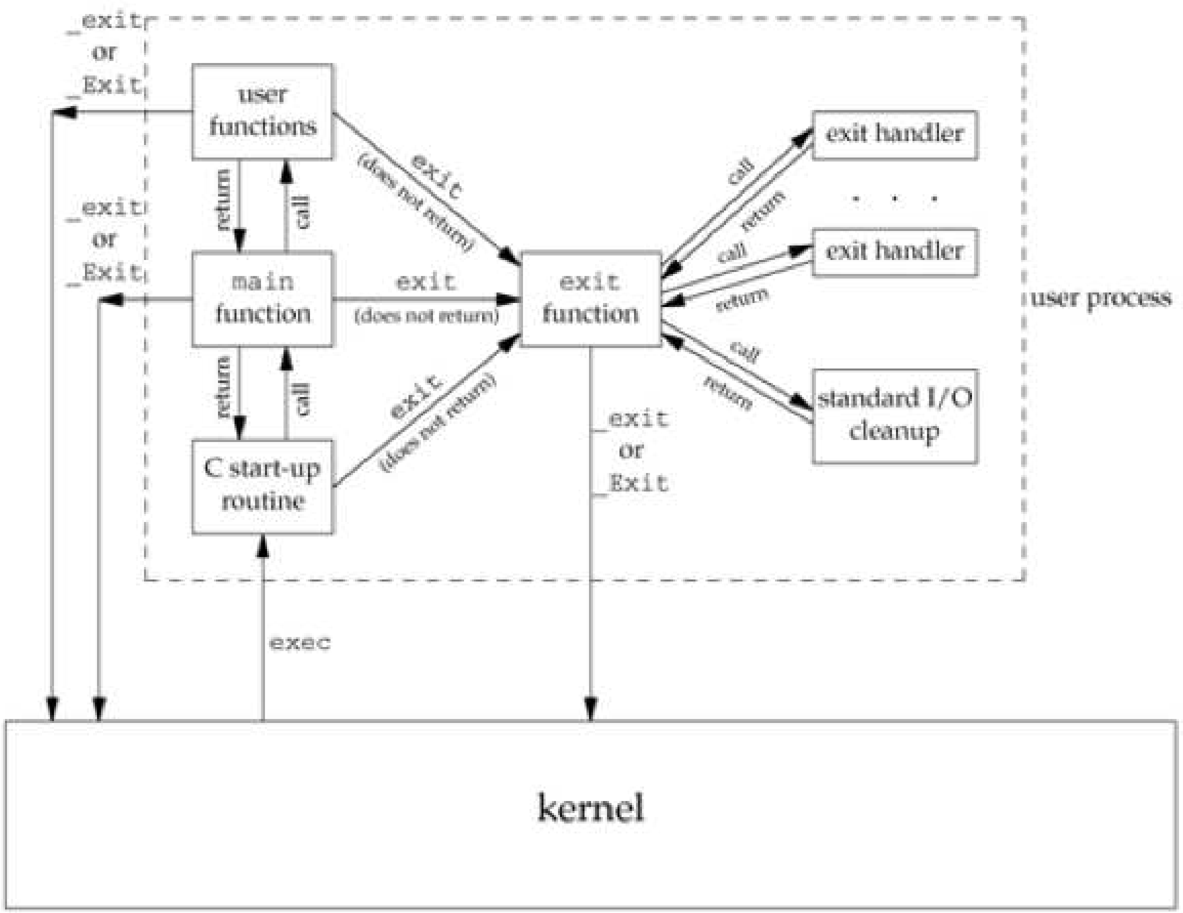
atexit(3)

```
#include <stdlib.h>

int atexit(void (*func)(void));
```

- Registers a function with a signature of `void funcname(void)` to be called at exit
- Functions invoked in reverse order of registration
- Same function can be registered more than once
- Extremely useful for cleaning up open files, freeing certain resources, etc.

`exit-handlers.c`

Lifetime of a UNIX Process



Exit codes

```
$ cc -Wall hw.c
hw.c: In function 'main':
hw.c:7: warning: control reaches end of non-void function
$ ./a.out
Hello World!
$ echo $?
10
$
```

Environment List

Environment variables are stored in a global array of pointers:

```
extern char **environ;
```

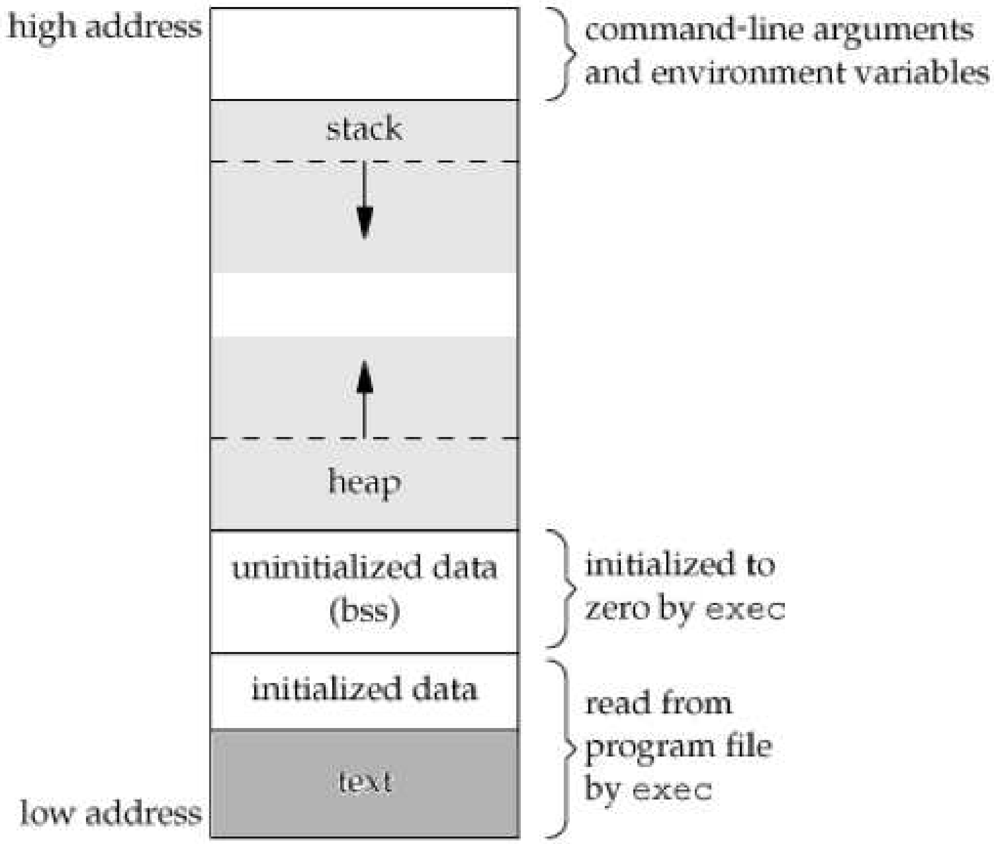
The list is `null` terminated.

These can also be accessed by:

```
#include <stdlib.h>


char *getenv(const char *name);
int putenv(const char *string);
int setenv(const char *name, const char *value, int rewrite);
void unsetenv(cont char *name);
```

```
int main(int argc, char **argv, char **anvp);
```

Memory Layout of a C Program



Memory Allocation

```
#include <stdlib.h>

void *malloc(size_t size);
void *calloc(size_t nobj, size_t size);
void *realloc(void *ptr, size_t newsize);
void *alloca(size_t size);

void free(void *ptr);
```

- *malloc* – initial value is indeterminate.
- *calloc* – initial value set to all zeros.
- *realloc* – changes size of previously allocated area. Initial value of any additional space is indeterminate.
- *alloca* – allocates memory on stack

Memory Allocation

Did you know?

`malloc(3)` can fail. Really!

Process limits

```
$ ulimit -a
time(cpu-seconds)    unlimited
file(blocks)         unlimited
coredump(blocks)     unlimited
data(kbytes)         262144
stack(kbytes)        2048
lockedmem(kbytes)    249913
memory(kbytes)       749740
nofiles(descriptors) 128
processes            160
vmemory(kbytes)      unlimited
sbsize(bytes)        unlimited
$
```

Process Identifiers

```
#include <unistd.h>

pid_t getpid(void);
pid_t getppid(void);
```

Process ID's are guaranteed to be unique and identify a particular executing process with a non-negative integer.

Certain processes have fixed, special identifiers. They are:

- *swapper*, process ID 0 – responsible for scheduling
- *init*, process ID 1 – bootstraps a Unix system, owns orphaned processes
- *pagedaemon*, process ID 2 – responsible for the VM system (some Unix systems)

fork(2)

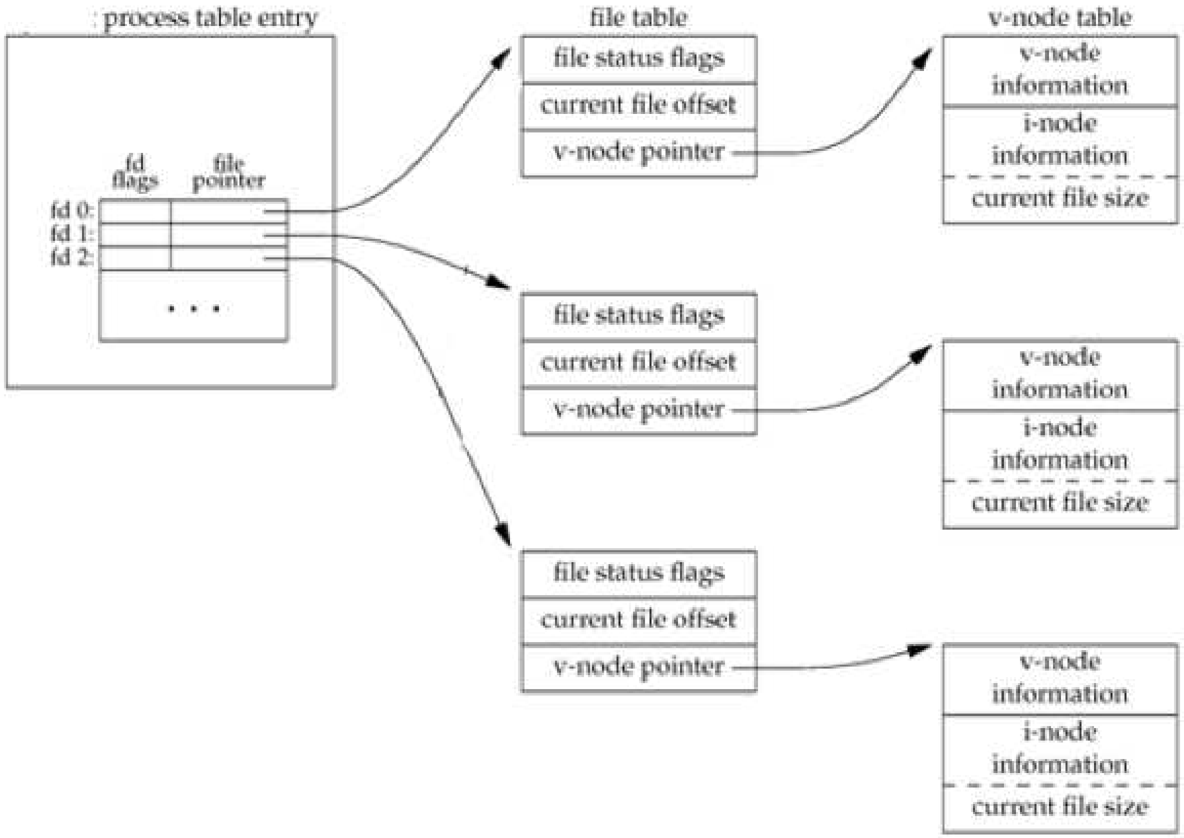
```
#include <unistd.h>

pid_t fork(void);
```

fork(2) causes creation of a new process. The new process (child process) is an exact copy of the calling process (parent process) except for the following:

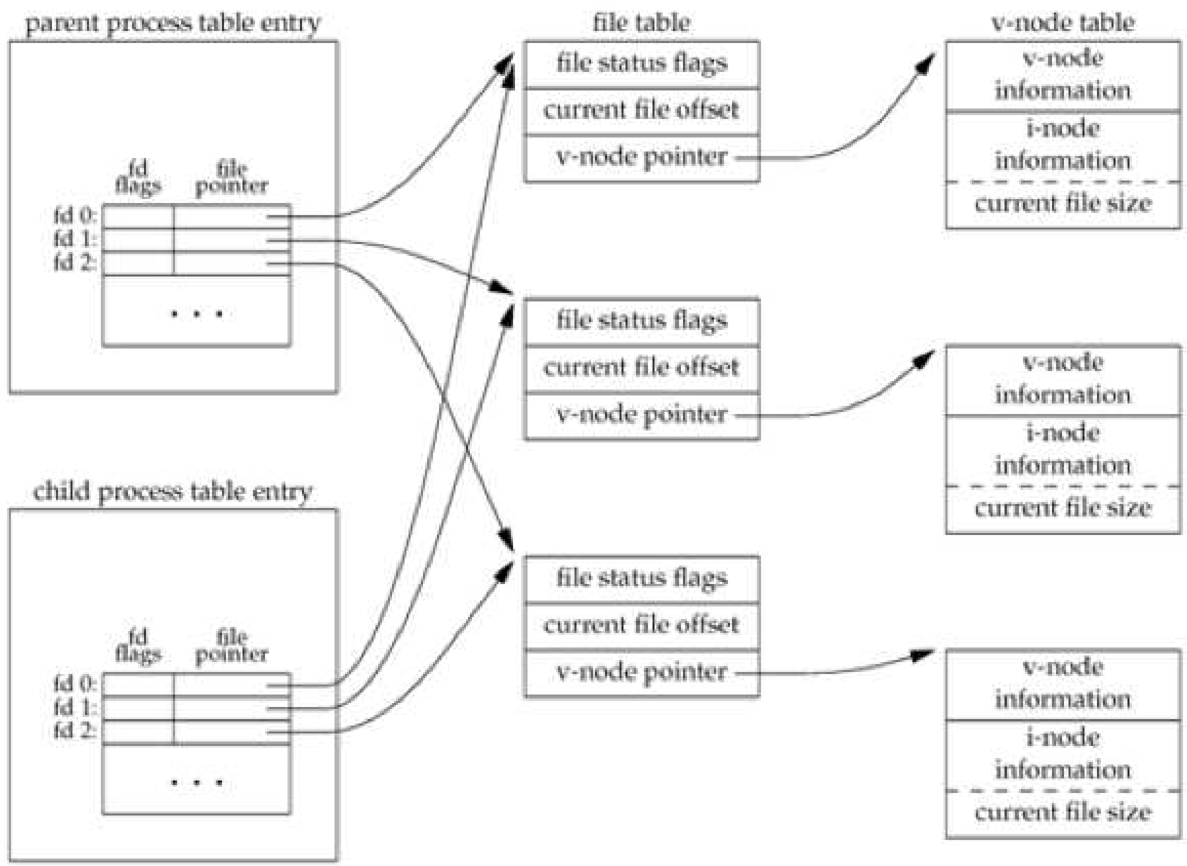
- The child process has a unique process ID.
- The child process has a different parent process ID (i.e., the process ID of the parent process).
- The child process has its own copy of the parent's descriptors.
- The child process' resource utilizations are set to 0.

Note: no order of execution between child and parent is guaranteed!

fork(2)


process table entry
fd flags
file pointer
fd 0:
fd 1:
fd 2:
. . .
file table
file status flags
current file offset
v-node pointer
file status flags
current file offset
v-node pointer
file status flags
current file offset
v-node pointer
v-node table
v-node information
i-node information
current file size
v-node information
i-node information
current file size
v-node information
i-node information
current file size

fork(2)


parent process table entry
fd flags
file pointer
fd 0:
fd 1:
fd 2:
. . .
child process table entry
fd flags
file pointer
fd 0:
fd 1:
fd 2:
. . .
file table
file status flags
current file offset
v-node pointer
file status flags
current file offset
v-node pointer
file status flags
current file offset
v-node pointer
v-node table
v-node information
i-node information
current file size
v-node information
i-node information
current file size
v-node information
i-node information
current file size

fork(2)

```
$ cc -Wall forkflush.c
$ ./a.out
a write to stdout
before fork
pid = 12149, glob = 7, var = 89
pid = 12148, glob = 6, var = 88
$ ./a.out | cat
a write to stdout
before fork
pid = 12153, glob = 7, var = 89
before fork
pid = 12151, glob = 6, var = 88
$
```

The exec(3) functions

```
#include <unistd.h>

int execl(const char *pathname, const char *arg0, ...  /* (char *) 0 */);

int execv(const char *pathname, char * const argvp[]);

int execle(const char *pathname, const char *arg0, ...  /* (char *) 0, char *const envp[] */ );

int execve(const char *pathname, char * const argvp[], char * const envp[]);

int execlp(const char *filename, const char *arg0, ...  /* (char *) 0 */);

int execvp(const char *filename, char *const argv[]);
```

The `exec()` family of functions are used to completely replace a running process with a a new executable.

- if it has a v in its name, argv's are a vector: `const * char argv[]`
- if it has an l in its name, argv's are a list: `const char *arg0, ... /* (char *) 0 */`
- if it has an e in its name, it takes a `char * const envp[]` array of environment variables
- if it has a p in its name, it uses the `PATH` environment variable to search for the file

wait(2) and waitpid(2)

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

pid_t wait(int *status);
pid_t waitpid(pid_t wpid, int *status, int options);
pid_t wait3(int *status, int options, struct rusage *rusage);
pid_t wait4(pid_t wpid, int *status, int options, struct rusage *rusage);
```

A parent that calls `wait(2)` or `waitpid(2)` can:

- block (if all of its children are still running)
- return immediately with the termination status of a child
- return immediately with an error

Lecture 06

Process Groups, Sessions, Signals

Login Process

Let's revisit the process relationships for a login:

kernel	⇒	init(8)	# explicit creation
init(8)	⇒	getty(8)	# fork(2)
getty(8)	⇒	login(1)	# exec(3)
login(1)	⇒	`$SHELL`	# exec(3)
`$SHELL`	⇒	ls(1)	# fork(2) + exec(3)

Login Process

init(8) # PID 1, PPID 0, EUID 0

getty(8) # PID *N*, PPID 1, EUID 0

login(1) # PID *N*, PPID 1, EUID 0

`$SHELL` # PID *N*, PPID 1, EUID *U*

ls(1) # PID *M*, PPID *N*, EUID *U*

```
pstree -hapun | more
```

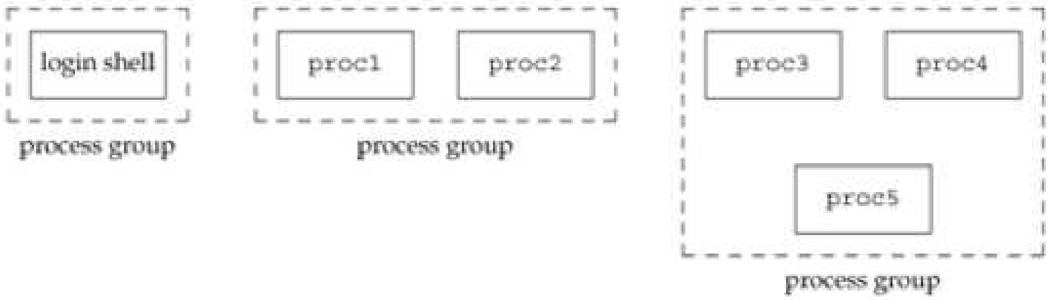
Process Groups

```
#include <unistd.h>

pid_t getpgrp(void);
pid_t getpgid(pid_t pid);
```

Returns: process group ID if OK, -1 otherwise

- in addition to having a PID, each process also belongs to a process group (collection of processes assocaited with the same job / terminal)
- each process group has a unique process group ID
- process group IDs (like PIDs) are positive integers and can be stored in a `pid_t` data type
- each process group can have a process group leader
  - leader identified by its process group ID == PID
  - leader can create a new process group, create processes in the group
- a process can set its (or its children's) process group using `setpgid(2)`

Process Groups



init ⇒ *login shell*

```
$ proc1 | proc2 &
[1] 10306
$ proc3 | proc4 | proc5
```

Process Groups and Sessions

```
#include <unistd.h>

pid_t setsid(void);
```

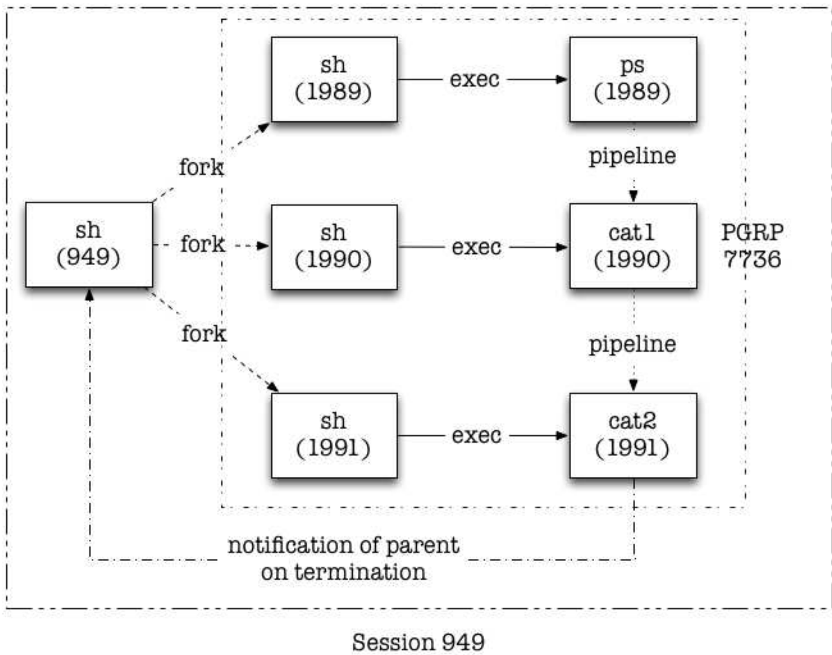
Returns: process group ID if OK, -1 otherwise

A session is a collection of one or more process groups.

If the calling process is not a process group leader, this function creates a new session. Three things happen:

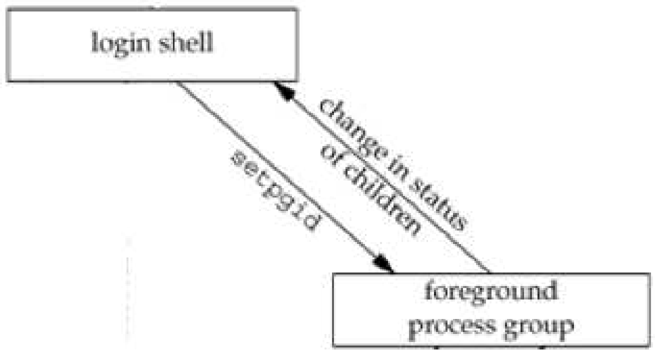
- the process becomes the session leader of this new session
- the process becomes the process group leader of a new process group
- the process has no controlling terminal

Process Groups and Sessions



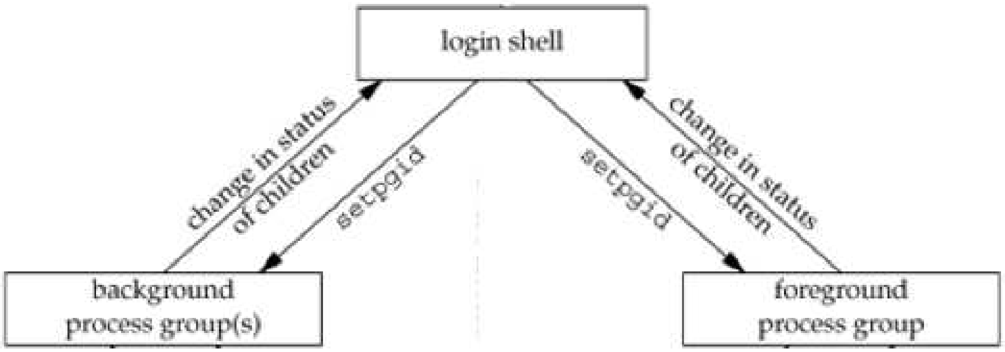

```
$ ps -o pid,ppid,pgid,sess,comm | ./cat1 | ./cat2
  PID  PPID  PGRP  SESS COMMAND
 1989   949  7736   949 ps
 1990   949  7736   949 cat1
 1988   949  7736   949 cat2
  949 21401   949   949 ksh
```

Job Control




```
$ ps -o pid,ppid,pgid,sess,comm
  PID  PPID  PGRP  SESS COMMAND
24251 24250 24251 24251 ksh
24620 24251 24620 24251 ps
$ echo $?
0
$
```

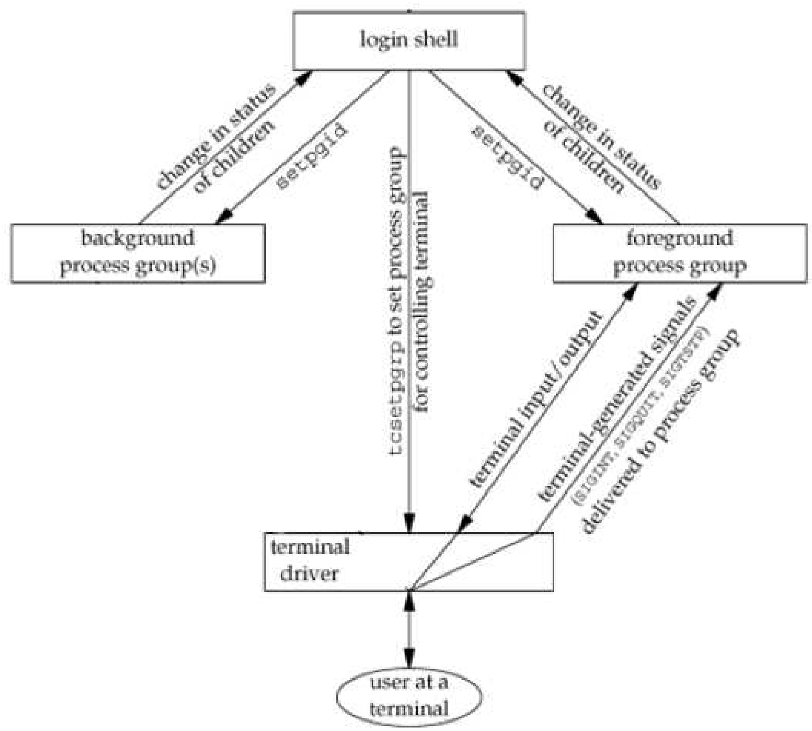
Job Control




```
$ dd if=/dev/zero of=/dev/null bs=512 count=2048000 >/dev/null 2>&1 &
[1] 24748
$ ps -o pid,ppid,pgid,sess,comm
  PID  PPID  PGRP  SESS COMMAND
24251 24250 24251 24251 ksh
24748 24251 24748 24251 dd
24750 24251 24750 24251 ps
$
[1] +  Done     dd if=/dev/zero of=/dev/null bs=512 count=2048000 >/dev/null 2>&1 &
$
```

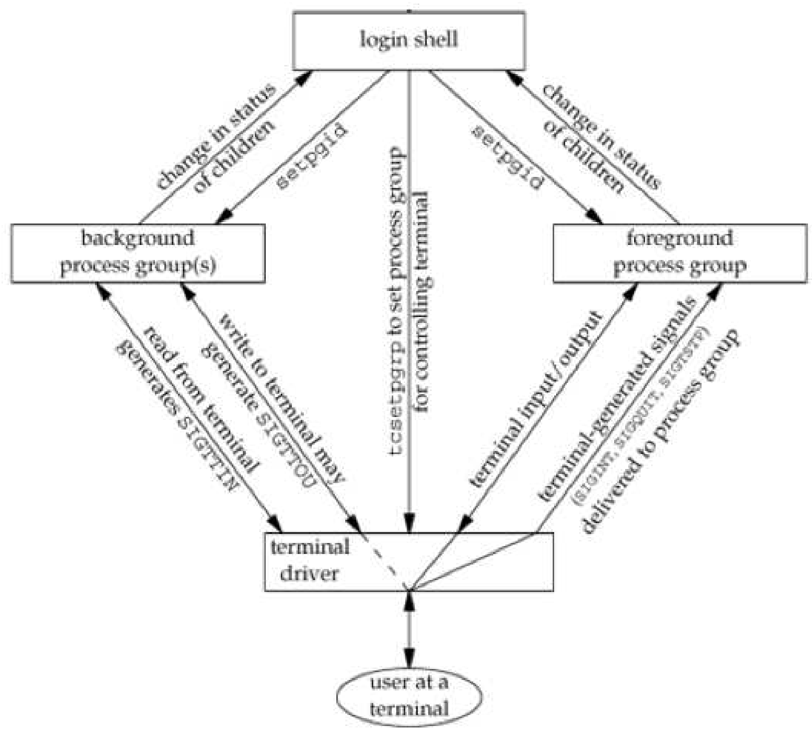
Job Control

```
$ cat >file
Input from terminal,
Output to terminal.
^D
$ cat file
Input from terminal,
Output to terminal.
$ cat >/dev/null
Input from terminal,
Output to /dev/null.
Waiting forever...
Or until we send an interrupt signal.
^C
$
```



Job Control

```
$ cat file &
[1] 2056
$ Input from terminal,
Output to terminal.

[1] +  Done                cat file &
$ stty tostop
$ cat file &
[1] 4655
$
[1] + Stopped(SIGTTOU)  cat file &
$ fg
cat file
Input from terminal,
Output to terminal.
$
```



Signals

Signal Concepts

Signals are a way for a process to be notified of asynchronous events. Some examples:

- a timer you set has gone off (`SIGALRM`)
- some I/O you requested has occurred (`SIGIO`)
- a user resized the terminal "window" (`SIGWINCH`)
- a user disconnected from the system (`SIGHUP`)
- ...

See also: `signal(2)/signal(3)/signal(7)` (note: these man pages vary significantly across platforms!)

Signal Concepts

Besides the asynchronous events listed previously, there are many ways to generate a signal:

- terminal generated signals (user presses a key combination which causes the terminal driver to generate a signal)
- hardware exceptions (divide by 0, invalid memory references, etc)
- `kill(1)` allows a user to send any signal to any process (if the user is the owner or superuser)
- `kill(2)` (a system call, not the unix command) performs the same task
- software conditions (other side of a pipe no longer exists, urgent data has arrived on a network file descriptor, etc.)

kill(2) and raise(3)

```
#include <sys/types.h>
#include <signal.h>

int kill(pid_t pid, int signo);
int raise(int signo);
```

- *pid* $>$ *0* – signal is sent to the process whose PID is `pid`
- *pid == 0* – signal is sent to all processes whose process group ID equals the process group ID of the sender
- *pid == -1* – POSIX.1 leaves this undefined, BSD defines it (see `kill(2)`)

Signal Concepts

Once we get a signal, we can do one of several things:

- Ignore it. (note: there are some signals which we CANNOT or SHOULD NOT ignore)
- Catch it. That is, have the kernel call a function which we define whenever the signal occurs.
- Accept the default. Have the kernel do whatever is defined as the default action for this signal

signal(3)

```
#include <signal.h>

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

Returns: previous disposition of signal if OK, SIG_ERR otherwise

func can be:

- SIG_IGN which requests that we ignore the signal signo
- SIG_DFL which requests that we accept the default action for signal signo
- or the address of a function which should catch or handle a signal

Interrupted System Calls

Some system calls can block for long periods of time (or forever). These include things like:

- `read(2)`s from files that can block (pipes, networks, terminals)
- `write(2)` to the same sort of files
- `open(2)` of a device that waits until a condition occurs (for example, a modem)
- `pause(3)`, which purposefully puts a process to sleep until a signal occurs
- certain `ioctl(3)`s
- certain IPC functions

Catching a signal during execution of one of these calls traditionally led to the process being aborted with an errno return of `EINTR`.

Lecture 07

Interprocess Communications

Pipes: `pipe(2)`

```
#include <unistd.h>

int pipe(int filedes[2]);
```

Returns: 0 if OK, -1 otherwise

- oldest and most common form of UNIX IPC
- half-duplex (on some versions full-duplex)
- can only be used between processes that have a common ancestor
- can have multiple readers/writers (`PIPE_BUF` bytes are guaranteed to not be interleaved)

Behavior after closing one end:

- `read(2)` from a pipe whose write end has been closed returns 0 after all data has been read
- `write(2)` to a pipe whose read end has been closed generates `SIGPIPE` signal. If caught or ignored, `write(2)` returns an error and sets `errno` to `EPIPE`.

Pipes: `popen(3)` and `pclose(3)`

```
#include <stdio.h>

FILE *popen(const char *cmd, const char *type);
```

Returns: file pointer if OK, `NULL` otherwise

```
int pclose(FILE *fp);
```

Returns: termination status *cmd* or -1 on error

- historically implemented using unidirectional pipe (nowadays frequently implemented using sockets or full-duplex pipes)
- *type* one of “r” or “w” (or “r+” for bi-directional communication, if available)
- *cmd* passed to `/bin/sh -c`

FIFOs: `mkfifo(2)`

```
#include <sys/stat.h>

int mkfifo(const char *path, mode_t mode);
```

Returns: 0 if OK, -1 otherwise

- aka "named pipes"
- allows unrelated processes to communicate
- just a type of file – test for using `S_ISFIFO(st_mode)`
- *mode* same as for `open(2)`
- use regular I/O operations (ie `open(2)`, `read(2)`, `write(2)`, `unlink(2)` etc.)
- used by shell commands to pass data from one shell pipeline to another without creating intermediate temporary files

System V IPC

Three types of IPC originating from System V:

- Semaphores
- Shared Memory
- Message Queues

All three use *IPC structures*, referred to by an *identifier* and a *key*; all three are (necessarily) limited to communication between processes on one and the same host. All allow for *asynchronous* communication.

Since these structures are not known by name, special system calls (`msgget(2)`, `semop(2)`, `shmat(2)`, etc.) and special userland commands (`ipcrm(1)`, `ipcs(1)`, etc.) are necessary.

Sockets: `socket(2)`

```
#include <sys/socket.h>

int socket(int domain, int type, int protocol);
```

Some of the currently supported domains are:

Domain	Description
PF_LOCAL	local (previously UNIX) domain protocols
PF_INET	ARPA Internet protocols
PF_INET6	ARPA IPv6 (Internet Protocol version 6) protocols
PF_ARP	RFC 826 Ethernet Address Resolution Protocol
...	...

Some of the currently defined types are:

Type	Description
SOCK_STREAM	sequenced, reliable, two-way connection based byte streams
SOCK_DGRAM	connectionless, unreliable messages of a fixed (typically small) maximum length
SOCK_RAW	access to internal network protocols and interfaces
...	...

Sockets: Datagrams in the UNIX/LOCAL domain

- create socket using `socket(2)`
- attach to a socket using `bind(2)`
- binding a name in the UNIX domain creates a socket in the file system
- both processes need to agree on the name to use
- these files are only used for rendezvous, not for message delivery once a connection has been established
- sockets must be removed using `unlink(2)`

Sockets: Datagrams in the Internet Domain

- Unlike UNIX domain names, Internet socket names are not entered into the file system and, therefore, they do not have to be unlinked after the socket has been closed.
- The local machine address for a socket can be any valid network address of the machine, if it has more than one, or it can be the wildcard value `INADDR_ANY`.
- “well-known” ports (range 1 - 1023) only available to super-user
- request any port by calling `bind(2)` with a port number of 0
- determine used port number (or other information) using `getsockname(2)`
- convert between network byteorder and host byteorder using `htons(3)` and `ntohs(3)` (which may be noops)

Sockets: Connections using stream sockets

- connections are asymmetrical: one process requests a connection, the other process accepts the request
- one socket is created for each accepted request
- mark socket as willing to accept connections using `listen(2)`
- pending connections are then `accept(2)`ed
- `accept(2)` will block if no connections are available
- `select(2)` to check if connection requests are pending

Lecture 08

Advanced IO

Nonblocking I/O

Recall from our lecture on signals that certain system calls can block forever:

- `read(2)` from a particular file, if data isn't present (pipes, terminals, network devices)
- `write(2)` to the same kind of file
- `open(2)` of a particular file until a specific condition occurs
- `read(2)` and `write(2)` of files that have mandatory locking enabled
- certain `ioctls(2)`
- some IPC functions (such as `sendto(2)` or `recv(2)`)

Nonblocking I/O lets us issue an I/O operation and not have it block forever. If the operation cannot be completed, return is made immediately with an error noting that the operating would have blocked (`EWOULDBLOCK` or `EAGAIN`).

Advisory Locking

```
#include <fcntl.h>

int flock(int fd,int operation);
```

Returns: 0 if OK, -1 otherwise

- applies or removes an advisory lock on the file associated with the file descriptor fd
- *operation* can be `LOCK_NB` and any one of:
  - `LOCK_SH`
  - `LOCK_EX`
  - `LOCK_UN`
- locks entire file

Advisory “Record” locking

```
#include <unistd.h>

int lockf(int fd, int value, off_t size);
```

Returns: 0 on success, -1 on error

value can be:

- `F_ULOCK` – unlock locked sections
- `F_LOCK` – lock a section for exclusive use
- `F_TLOCK` – test and lock a section for exclusive use
- `F_TEST` – test a section for locks by other processes

		Request for	
		read lock	write lock
Region currently has	no locks	OK	OK
	one or more read locks	OK	denied
	one write lock	denied	denied

Mandatory locking

- not implemented on all UNIX flavors
  - `chmod g+s,g-x file`
- possible to be circumvented:

```
$ mandatory-lock /tmp/file &
$ echo foo > /tmp/file2
$ rm /tmp/file
$ mv /tmp/file2 /tmp/file
```

See also:
`https://www.kernel.org/doc/Documentation/filesystems/mandatory-locking.txt`

I/O Multiplexing

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

int select(int maxfdp1, fd_set *readfds, fd_set *writefds
               fd_set *exceptfds, struct timeval *tvptr);
```

Returns: count of ready descriptors, 0 on timeout, -1 otherwise

Arguments passed:

- which descriptors we're interested in
- what conditions we're interested in
- how long we want to wait
  - `tvptr == NULL` means wait forever
  - `tvptr->tv_sec == tvptr->tv_usec == 0` means don't wait at all
  - wait for specified amount of time

`select(2)` tells us both the total count of descriptors that are ready as well as which ones are ready.

Memory Mapped I/O

```
#include <sys/types.h>
#include <sys/mman.h>

void *mmap(void *addr, size_t len, int prot, int flags, int fd, off_t offset);
```

Returns: pointer to mapped region if OK

Protection specified for a region:

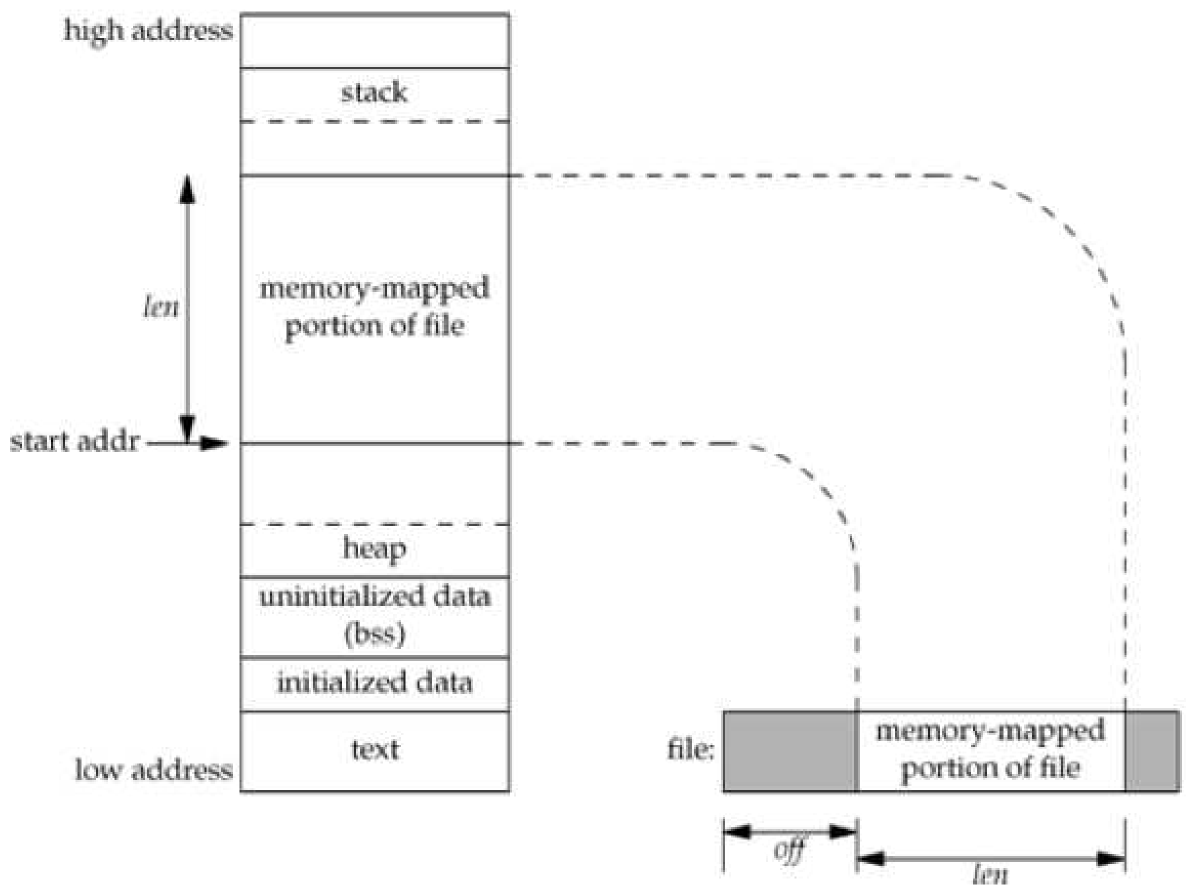
- `PROT_READ` – region can be read
- `PROT_WRITE` – region can be written
- `PROT_EXEC` – region can be executed
- `PROT_NONE` – region can not be accessed

flag needs to be one of

- `MAP_SHARED`
- `MAP_PRIVATE`
- `MAP_COPY`

which may be OR'd with other flags (see `mmap(2)` for details).

Memory Mapped I/O



Lecture 09

Dæmon processes, System Logging, Shared Libraries

Dæmon characteristics

Commonly, dæmon processes are created to offer a specific service.

Dæmon processes usually

- live for a long time
- are started at boot time
- terminate only during shutdown
- have no controlling terminal

Dæmon characteristics

The previously listed characteristics have certain implications:

- do one thing, and one thing only
- no (or only limited) user-interaction possible
- consider current working directory
- how to create (debugging) output

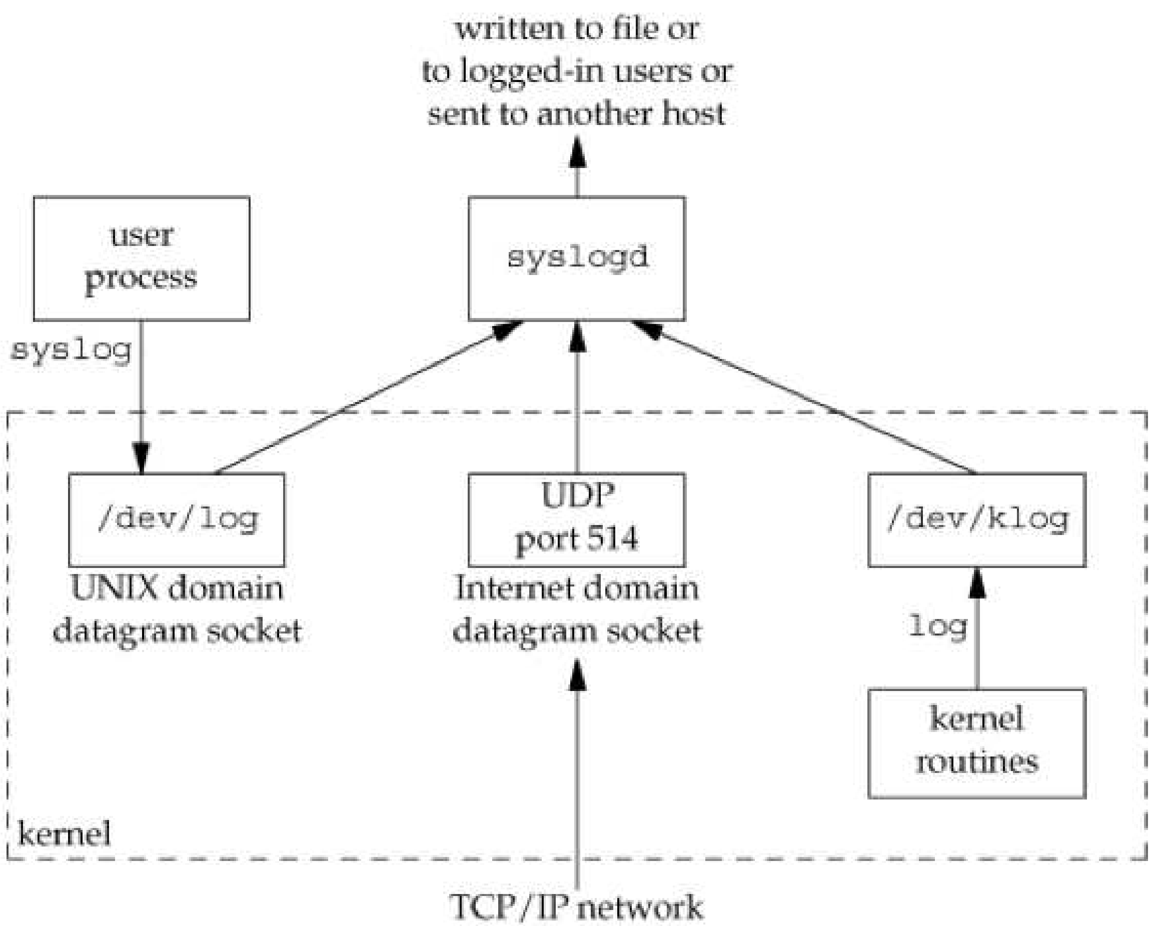
Writing a dæmon

- fork off the parent process
- change file mode mask (umask)
- create a unique Session ID (SID)
- change the current working directory to a safe place
- close (or redirect) standard file descriptors
- open any logs for writing
- enter actual dæmon code

Writing a dæmon

```
int
daemon(int nochdir, int noclose)
{
        int fd;

        switch (fork()) {
        case -1:
                return (-1);
        case 0:
                break;
        default:
                _exit(0);
        }

        if (setsid() == -1)
                return (-1);

        if (!nochdir)
                (void)chdir("/");

        if (!noclose && (fd = open(_PATH_DEVNULL, O_RDWR, 0)) != -1) {
                (void)dup2(fd, STDIN_FILENO);
                (void)dup2(fd, STDOUT_FILENO);
                (void)dup2(fd, STDERR_FILENO);
                if (fd > STDERR_FILENO)
                        (void)close(fd);
        }
        return (0);
}
```

A central logging facility



syslog(3)

```
#include <syslog.h>

void openlog(const char *ident, int logopt, int facility);
void syslog(int priority, const char *message, ...);
```

`openlog(3)` allows us to set specific options when logging:

- prepend *ident* to each message
- specify logging options (`LOG_CONS | LOG_NDELAY | LOG_PERROR | LOG_PID`)
- specify a *facility* (such as `LOG_DAEMON`, `LOG_MAIL` etc.)

`syslog(3)` writes a message to the system message logger, tagged with *priority*.
A *priority* is a combination of a *facility* (as above) and a *level* (such as `LOG_DEBUG`, `LOG_WARNING` or `LOG_EMERG`).

Shared Libraries

What is a shared library, anyway?

- contains a set of callable C functions (ie, implementation of function prototypes defined in `.h` header files)
- code is position-independent (ie, code can be executed anywhere in memory)
- shared libraries can be loaded/unloaded at execution time or at will
- libraries may be *static* or *dynamic*

```
$ man 3 fprintf
$ grep " fprintf" /usr/include/stdio.h
```

Shared Libraries

How do shared libraries work?

- contents of *static* libraries are pulled into the executable at link time
- contents of *dynamic* libraries are used to resolve symbols at **link time**, but loaded at **execution time** by the *dynamic linker*
- contents of *dynamic* libraries may be loaded at **any time** via explicit calls to the dynamic linking loader interface functions

Understanding object files

```
$ cc -Wall -c ldtest1.c ldtest2.c main.c
$ readelf -h ldtest1.o
[...]
$ cc *.o
$ readelf -h a.out
[...]
$ ldd a.out
[...]
$ readelf -h /lib/x86_64-linux-gnu/libc.so.6
[...]
$ readelf -s a.out | more
[...]
$ objdump -d -j .text a.out | more
[...]
$ nm -D a.out | more
[...]
$
```

Statically Linked Shared Libraries

Static libraries:

- created by `ar(1)`
- usually end in `.a`
- contain a symbol table within the archive (see `ranlib(1)`)

Statically Linked Shared Libraries

```
$ cc -Wall -c ldtest1.c ldtest2.c
$ ar -vq libldtest.a ldtest1.o ldtest2.o
$ ar -t libldtest.a
$ cc -Wall main.c libldtest.a

$ cc -Wall -c main.c
$ cc main.o -L. -lldtest -o a.out.dyn
$ cc -static main.o -L. -lldtest -o a.out.static
$ ls -l a.out.*
$ ldd a.out.*
$ nm a.out.dyn | wc -l
$ nm a.out.static | wc -l
```

Dynamically Linked Shared Libraries

Explicit loading of shared libraries:

- `dlopen(3)` creates a handle for the given library
- `dlsym(3)` returns the address of the given symbol
-

```
$ cc -Wall setget.c
$ cc -Wall -rdynamic dlopenex.c -ldl
$ ./a.out
```

Dynamically Linked Shared Libraries

Dynamic libraries:

- created by the compiler/linker (ie multiple steps)
- usually end in `.so`
- frequently have multiple levels of symlinks providing backwards compatibility / ABI definitions

Dynamically Linked Shared Libraries

```
$ rm *.o libldtest*
$ cc -Wall -c -fPIC ldtest1.c
$ cc -Wall -c -fPIC ldtest2.c
$ mkdir lib
$ cc -shared -Wl,-soname,libldtest.so.1 -o lib/libldtest.so.1.0 ldtest1.o ldtest2.o
$ ln -s libldtest.so.1.0 lib/libldtest.so.1
$ ln -s libldtest.so.1.0 lib/libldtest.so
$ cc -static -Wall main.o -L./lib -lldtest
[...]
$ cc -Wall main.o -L./lib -lldtest
[...]
$ ./a.out
[...]
$ ldd a.out
[...]
```

Dynamically Linked Shared Libraries

Wait, what?

```
$ LD_LIBRARY_PATH=./lib ldd a.out
[...]
$ LD_LIBRARY_PATH=./lib ./a.out
[...]
$ mkdir lib2
$ cc -Wall -c -fPIC ldtest1.2.c
$ cc -shared -Wl,-soname,libldtest.so.1 -o lib2/libldtest.so.1.0 ldtest1.2.o ldtest2.
$ ln -s libldtest.so.1.0 lib2/libldtest.so.1
$ ln -s libldtest.so.1.0 lib2/libldtest.so
$ LD_LIBRARY_PATH=./lib2 ldd a.out  # note: no recompiling!
[...]
$ LD_LIBRARY_PATH=./lib ./a.out
$ LD_LIBRARY_PATH=./lib2 ./a.out
[...]
```

Dynamically Linked Shared Libraries

Avoiding `LD_LIBRARY_PATH`:

```
$ cc -Wall main.o -L./lib -llldtest -Wl,-rpath,./lib
$ ldd a.out
[...]
$ ./a.out
[...]
$ LD_LIBRARY_PATH=./lib2 ./a.out
[...]
$
```

Dynamically Linked Shared Libraries

But:

```
$ cc -Wall -fPIC -c evil.c
$ cc -shared -Wl,-soname,libldtest.so.1 -o lib3/libldtest.so.1.0 \
        ldtest1.o ldtest2.o evil.o
$ export LD_PRELOAD=./lib3/libldtest.so.1.0
$ ldd a.out
[...]
$ ./a.out
[...]
$
```

Lecture 10

UNIX Development Tools

Software Development Tools

UNIX Userland is an IDE – essential tools that follow the paradigm of "Do one thing, and do it right" can be combined.

The most important tools are:

- `$EDITOR`
- the compiler toolchain
- `gdb(1)` – debugging your code
- `make(1)` – project build management, maintain program dependencies
- `diff(1)` and `patch(1)` – report and apply differences between files
- `cvs(1)`, `svn(1)`, `git(1)` etc. – distributed project management, version control

Compilers

A compiler translates *source code* from a high-level programming language into *machine code* for a given architecture by performing a number of steps:

- lexical analysis
- preprocessing
- parsing
- semantic analysis
- code generation
- code optimization

Preprocessing

The compiler usually performs preprocessing (via `cpp(1)`), compilation (`cc(1)`), assembly (`as(1)`) and linking (`ld(1)`).

```
$ cd compilechain
$ cat hello.c
$ man cpp
$ cpp hello.c hello.i
$ file hello.i
$ man cc
$ cc -v -E hello.c > hello.i
$ more hello.i
$ cc -v -DFOOD=\"Avocado\" -E hello.c > hello.i.2
$ diff -bu hello.i hello.i.2
```

Compilation

The compiler usually performs preprocessing (via `cpp(1)`), compilation (`cc(1)`), assembly (`as(1)`) and linking (`ld(1)`).

```
$ more hello.i
$ cc -v -S hello.i > hello.s
$ file hello.s
$ more hello.s
```

Assembly

The compiler usually performs preprocessing (via `cpp(1)`), compilation (`cc(1)`), assembly (`as(1)`) and linking (`ld(1)`).

```
$ as -o hello.o hello.s
$ file hello.o
$ cc -v -c hello.s
$ objdump -d hello.o
[...]
```

Linking

The compiler usually performs preprocessing (via `cpp(1)`), compilation (`cc(1)`), assembly (`as(1)`) and linking (`ld(1)`).

```
$ ld hello.o
[...]
$ ld hello.o -lc
[...]
$ cc -v hello.o
[...]
$ ld -dynamic-linker /lib64/ld-linux-x86-64.so.2 \
        /usr/lib/x86_64-linux-gnu/crt1.o         \
        /usr/lib/x86_64-linux-gnu/crti.o hello.o \
        -lc /usr/lib/x86_64-linux-gnu/crtn.o
$ file a.out
$ ./a.out
```

`gdb(1)`

The purpose of a debugger such as `gdb(1)` is to allow you to see what is going on “inside” another program while it executes – or what another program was doing at the moment it crashed. `gdb` allows you to

- make your program stop on specified conditions (for example by setting *breakpoints*)
- examine what has happened, when your program has stopped (by looking at the *backtrace*, inspecting the value of certain variables)
- inspect control flow (for example by *stepping* through the program)

Other interesting things you can do:

- examine stack frames: *info frame*, *info locals*, *info args*
- examine memory: *x*
- examine assembly: *disassemble func*

gdb(1)

```
$ cd test
$ ./ls -lR ~djd >/dev/null
[...]
Memory fault
$ gdb ./ls
 run -lR ~djd
Starting program: /home/jschauma/apue/10/test/ls -lR ~djd
[...]

Program received signal SIGSEGV, Segmentation fault.
0x000000000040214a in print_entries (entryvect=0x6050a0, options=0x605010) at ls.c:
575                     if(gidlen < (temp = strlen(gp->gr_name)))
```

gdb(1)

```
(gdb) bt
#0  0x00000000004027a8 in print (ps=0x606290, ls=0x644f40) at ls.c:575
#1  0x0000000000402e1c in ls (argc=1, argv=0x7fffffffe9e8) at ls.c:707
#2  0x00000000004032a7 in main (argc=1, argv=0x7fffffffe9e8) at ls.c:858
(gdb) li
570                 else{
571                     pw = getpwuid(i->fts_statp->st_uid);
572                     gp = getgrgid(i->fts_statp->st_gid);
573                     if(uidlen < (temp = strlen(pw->pw_name)))
574                         uidlen = temp;
575                     if(gidlen < (temp = strlen(gp->gr_name)))
576                         gidlen = temp;
577                 }
578             }
579
(gdb) p gp
$1 = (struct group *) 0x0
```

`make(1)`

`make(1)` is a command generator and build utility. Using a description file (usually *Makefile*) it creates a sequence of commands for execution by the shell.

- used to sort out dependency relations among files
- avoids having to rebuild the entire project after modification of a single source file
- performs *selective* rebuilds following a *dependency graph*
- allows simplification of rules through use of *macros* and *suffixes*, some of which are internally defined
- different versions of `make(1)` (BSD make, GNU make, Sys V make, ...) may differ (among other things) in
  - variable assignment and expansion/substitution
  - including other files
  - flow control (for-loops, conditionals etc.)

`diff(1)` and `patch(1)`

`diff(1)`:

- compares files line by line
- output may be used to automatically edit a file
- can produce human “readable” output as well as diff entire directory structures
- output called a *patch*

`diff(1)` and `patch(1)`

`patch(1)`:

- applies a `diff(1)` file (aka *patch*) to an original
- may back up original file
- may guess correct format
- ignores leading or trailing “garbage”
- allows for reversing the patch
- may even correct context line numbers

Revision Control

Version control systems allow you to

- collaborate with others
- simultaneously work on a code base
- keep old versions of files
- keep a log of the who, when, what, and why of any changes
- perform release engineering by creating *branches*

Revision Control

- Source Code Control System (*SSCS*) begat the Revision Control System (*RCS*).
- RCS operates on a single file; still in use for misc. OS config files
- the Concurrent Versions System (*CVS*) introduces a client-server architecture, control of hierarchies
- *Subversion* provides atomic commits, renaming, cheap branching etc.
- *Git*, *Mercurial* etc. implement a *distributed* approach (ie peer-to-peer versus client-server), adding other features (cryptographic authentication of history, ...)

Lecture 12

Ecnryption Basics

Purpose of Encryption

Encryption provides security in the areas of:

- Authenticity
  - *Is the party I'm talking to actually who I* think *it is?*
- Accuracy or Integrity
  - *Is the message I received in fact what was sent?*
- Secrecy or Confidentiality
  - *Did/could anybody else see (parts of) the message?*

Authenticity

- in private key cryptography, authenticity is (often) assumed/implied
- in public key cryptography, often accomplished via a separate signature
- ways to establish assurance of authenticity for parties that have never met:
  - public key infrastructures (PKI) and certificate authorities (CA)
  - “web of trust”

Accuracy or Integrity

In order to protect against forgery or data manipulation, provide some sort of digest or checksum (often a one-way hash). Popular choices:

- `5f4dcc3b5aa765d61d8327deb882cf99` (MD5)
- `5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8` (SHA-1)
- `5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8` (SHA256)
- `b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86` (SHA512)

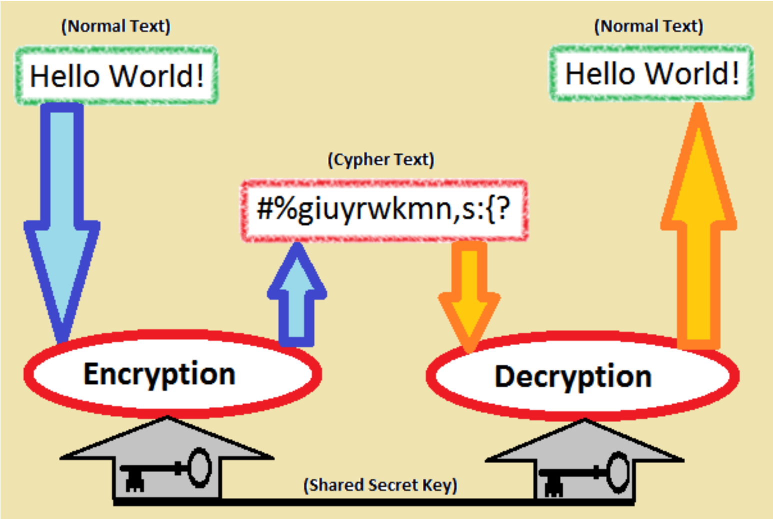
Caveats:

- "rainbow tables" / internet search engines allow for easy reverse lookup of un-salted hashes.
- integrity only ensured if authenticity of information itself is guaranteed

How does encryption work?

Secrecy: Make sure that the data can only be read by those intended.

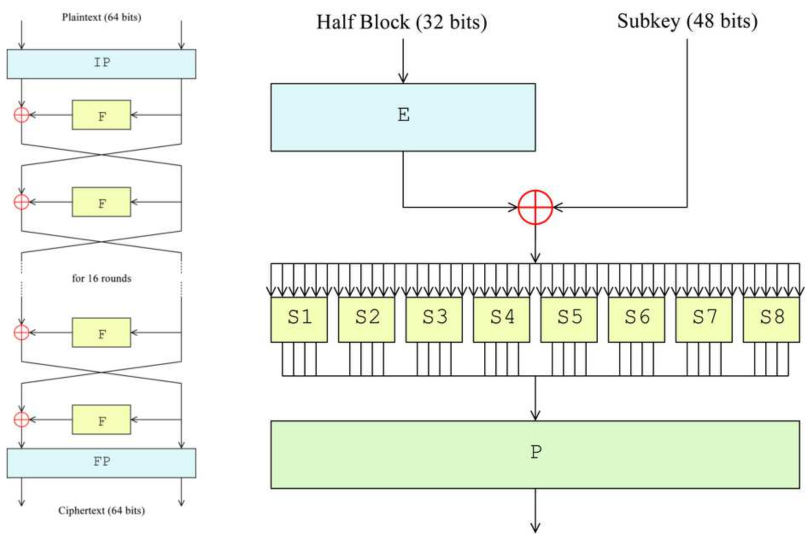
- Alice and Bob agree on a way to transform data
- transformed data is sent over insecure channel
- Alice and Bob are able to get data out of the transformation



How does encryption work?

Different approaches:

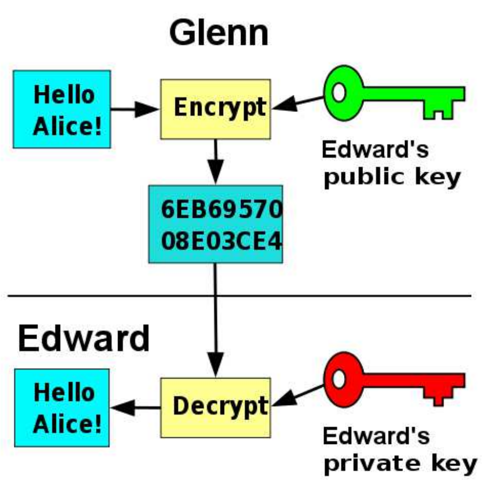
- secret key cryptography (example: *DES*)
  - Alice and Bob share a secret
  - Alice can prove to Bob that he knows a secret



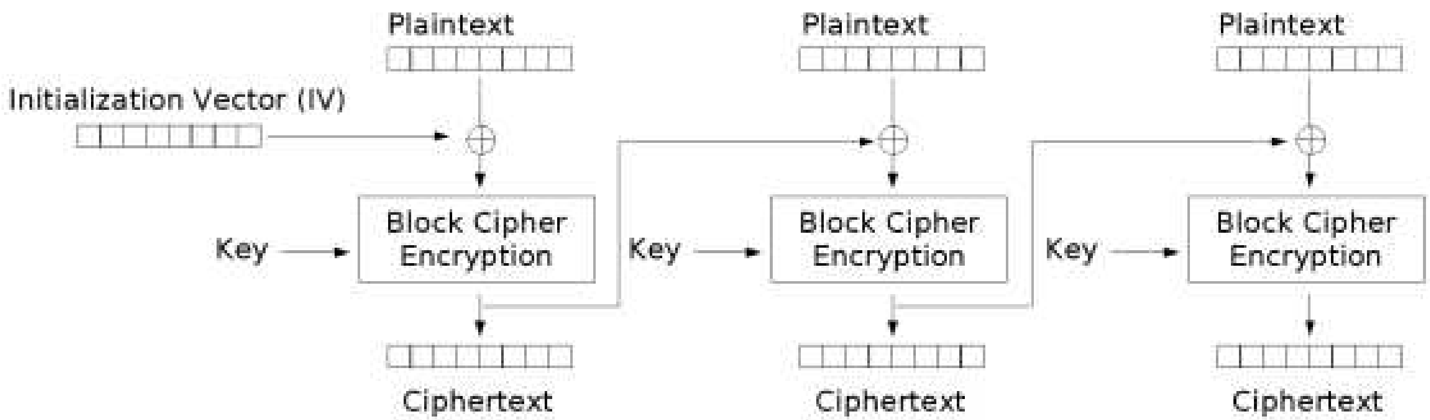
How does encryption work?

Different approaches:

- public key cryptography (example: *RSA*)
  - Alice has a private and a public key
  - data encrypted with her private key can only be decrypted by her public key and vice versa
  - public key can be shared with Bob

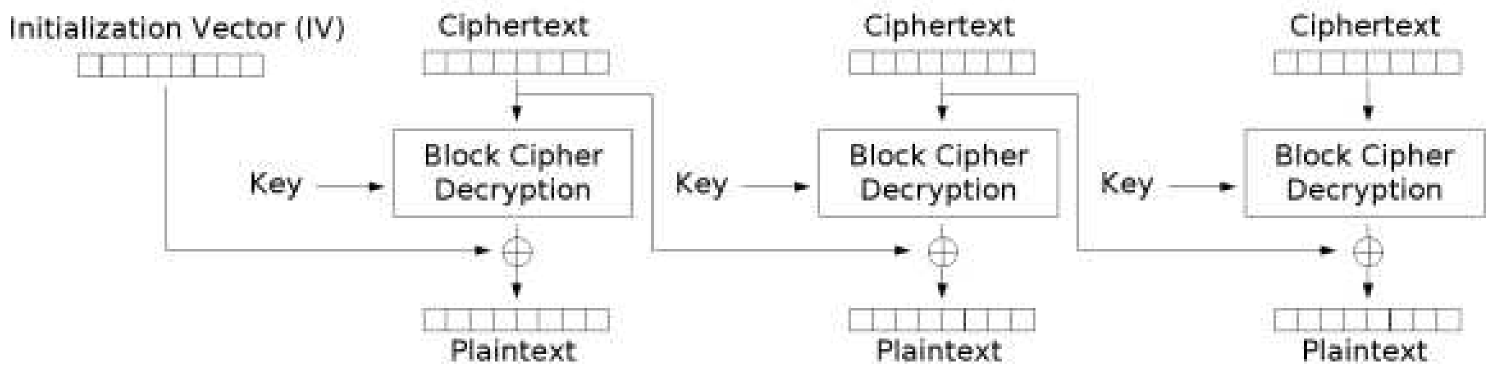


Cipher Block Chaining



Cipher Block Chaining (CBC) mode encryption

Cipher Block Chaining



Cipher Block Chaining (CBC) mode decryption

Practical AES

- a symmetric block cipher
- variable key length
- consists of a key setup phase and the actual encryption or decryption
- keying material use of `ivec`, which needs to be shared

Final Assignment

Write a simple shell.

`https://www.cs.stevens.edu/~jschauma/631/f14-sish.html`

That's all, folks!