CS 33

Libraries
Libraries

- Collections of useful stuff
- Incorporate items into your program
- Replace existing items with new stuff
- Often ugly ...
Files ending with "a" are known as *archives* or *static libraries*. 

```
$ gcc -c sub1.c sub2.c sub3.c
$ ls
sub1.c    sub2.c    sub3.c
sub1.o    sub2.o    sub3.o
$ ar cr libpriv1.a sub1.o sub2.o sub3.o
$ ar t libpriv1.a
sub1.o
sub2.o
sub3.o
$
```
The routine “puts” is from the standard-I/O library, just as printf is, but it’s far simpler. It prints its single string argument, appending a ‘\n’ (newline) to the end.

Note that “-lpriv1” (the second character of the string is a lower-case L and the last character is the numeral one) is, in this example, shorthand for libpriv1.a, but we’ll soon see that it’s shorthand for more than that.

Normally, libraries are expected to be found in the current directory. The “-L” flag is used to specify additional directories in which to look for libraries.
Static-Linking: What’s in the Executable

- **Id puts in the executable:**
  - (assume all .c files have been compiled into .o files)
  - all .o files from argument list (including those newly compiled)
  - .o files from archives as needed to satisfy unresolved references
    - some may have their own unresolved references that may need to be resolved from additional .o files from archives
    - each archive processed just once (as ordered in argument list)
      - order matters!
Example

```c
$ cat prog2.c
int main() {
    void func1();
    func1();
    return 0;
}
$ cat func1.c
void func1() {
    void func2();
    func2();
}
$ cat func2.c
void func2() {
}
```
Order Matters ...

$ ar t libf1.a
  func1.o
$ ar t libf2.a
  func2.o
$ gcc -o prog2 prog2.c -L. -lf1 -lf2
$
$ gcc -o prog2 prog2.c -L. -lf2 -lf1
  ./libf1.a(sub1.o): In function `func1':
  func1.c:(.text+0xa): undefined reference to `func2'
  collect2: error: ld returned 1 exit status
Substitution

```
$ cat myputs.c

int puts(char *s) {
    write(1, "My puts: ", 9);
    write(1, s, strlen(s));
    write(1, "\n", 1);
    return 1;
}

$ gcc -c myputs.c
$ ar cr libmyputs.a myputs.o
$ gcc -o prog prog.c -L -lpriv1 -lmyputs
$ ./prog

My puts: sub1
My puts: sub2
My puts: sub3
```
A Problem

- printf is found to have a bug
  - perhaps a security problem
- All existing instances must be replaced
  - there are zillions of instances ...
- Do we have to re-link all programs that use printf?
Dynamic Linking

- Executable is not fully linked
  - contains list of needed libraries
- Linkages set up when executable is run
Benefits

- **Without dynamic linking**
  - every executable contains copy of printf (and other stuff)
    - waste of disk space
    - waste of primary memory

- **With dynamic linking**
  - just one copy of printf
    - shared by all
Linux supports two kinds of libraries — static libraries, contained in *archives*, whose names end with “.a” (e.g. *libc.a*) and *shared* objects, whose names end with “.so” (e.g. *libc.so*). When *ld* is invoked to handle the linking of object code, it is normally given a list of libraries in which to find unresolved references. If it resolves a reference within a .a file, it copies the code from the file and statically links it into the object code. However, if it resolves the reference within a .so file, it records the name of the shared object (not the complete path, just the final component) and postpones actual linking until the program is executed.

If the program is fully bound and relocated, then it is ready for direct execution. However, if it is not fully bound and relocated, then *ld* arranges things so that when the program is executed, rather than starting with the program’s main routine, a runtime version of *ld*, called *ld-linux.so*, is called first. *ld-linux.so* maps all the required libraries into the address space and then calls the main routine.
The –fPIC flag tells gcc to produce "position-independent code," which is something we discuss soon. The ld command invokes the loader directly. The –shared flag tells it to created a shared object. In this case, it’s creating it from the object file myputs.o and calling the shared object libmyputs.so.

The error occurs because we haven’t indicated in the executable (prog) where ld-linux.so should look for shared objects. The ldd (list dynamic dependencies) command, which looks at all the shared objects referenced in the executable and prints out where they are found, shows us what the problem is.
The ‘-Wl,-rpath .‘ flag (the third character of the string is a lower-case L) tells the loader to indicate in the executable (prog) that ld-linux.so should look in the current directory (referred to as “.”) for shared objects. (The ‘-Wl‘ part of the flag tells gcc to pass the rest of the flag to the loader.)
Order Still Matters

- All shared objects listed in the executable are loaded into the address space
  - whether needed or not
- ld-linux.so will find anything that's there
  - looks in the order in which shared objects are listed
Here we are creating two versions of libmyputs, in libmyputs.so.1 and in libmyputs.so.2. Each is created by invoking the loader directly via the “ld” command. The “-soname” flag tells the loader to include in the shared object its name, which is the string following the flag (“libmyputs.so.1” in the first call to ld). The effect of the “ln –s” command is to create a new name (its last argument) in the file system that refers to the same file as that referred to by ln’s next-to-last argument. Thus, after the first call to ln –s, libmyputs.so refers to the same file as does libmyputs.so.1. Thus the second invocation of gcc, where it refers to –lmyputs (which expands to libmyputs.so), is actually referring to libmyputs.so.1.

Then we create a new version of myputs and from it a new shared object called libmyputs.so.2 (i.e., version 2). The call to “rm” removes the name libmyputs.so (but not the file it refers to, which is still referred to by libmyputs.so.1). Then ln is called again to make libmyputs.so now refer to the same file as does libmyputs.so.2. Thus when prog2 is linked, the reference to –lmyputs expands to libmyputs.so, which now refers to the same file as does libmyputs.so.2.

If prog1 is now run, it refers to libmyputs.so.1, so it gets the old version (version 1), but if prog2 is run, it refers to libmyputs.so.2, so it gets the new version (version 2). Thus programs using both versions of myputs can coexist.
Interpositioning

prog

wrapper

puts
How To ...

```c
int __wrap_puts(const char *s) {
    int __real_puts(const char *);

    write(2, "calling myputs: ", 16);
    return __real_puts(s);
}
```

__wrap_puts is the “wrapper” for puts. __real_puts is the “real” puts routine. What we want is for calls to puts to go to __wrap_puts, and calls to __real_puts to go to the real puts routine (in stdio).
The arguments to gcc shown in the slide cause what we asked for in the previous slide to actually happen. Calls to puts go to \_wrap\_puts, and calls to \_real\_puts go to the real puts routine.
An alternative approach to wrapping is to invoke ld-linux.so directly from the
program, and have it find the real puts routine. The call to dlsym above directly
invokes ld-linux.so, asking it (as given by the first argument) to find the next
definition of puts in the list of libraries. It returns the location of that routine,
which is then called (*pptr).
What’s Going On ...

- gcc/ld
  - compiles code
  - does static linking
    » searches list of libraries
    » adds references to shared objects

- runtime
  - program invokes ld-linux.so to finish linking
    » maps in shared objects
    » does relocation and procedure linking as required
  - dlsmv invokes ld-linux.so to do more linking
    » RTLD_NEXT says to use the next (second) occurrence of the symbol
Delayed Wrapping

- **LD_PRELOAD**
  - environment variable checked by *ld-linux.so*
  - specifies additional shared objects to search (first) when program is started
Example

```
$ gcc -o tputs tputs.c
$ ./tputs
This is a boring message.
$ LD_PRELOAD=./libmyputs.so.1; export LD_PRELOAD
$ ./tputs
calling myputs: This is a boring message.
$ 
```
Mmapping Libraries

available for mmap

stack

my lib

C library

dynamic

bss

data

text
Problem

• How is relocation handled?
Assuming we’re using pre-relocation, the C library and the math library would be assumed to be in virtual memory at their pre-assigned locations. In the slide, these would be starting at locations 1,000,000 and 3,000,000, respectively. Let’s suppose printf, which is in the C library, is at location 1,000,400. Thus calls to printf at static link time could be linked to that address. If the math library also contains calls to printf, these would be linked to that address as well. The C library might contain a global identifies, such as stdfiles. Its address would also be known.
Pre-relocation doesn’t work if we have two libraries pre-assigned such that they overlap. If so, at least one of the two will have to be moved, necessitating relocation.
But …

my library
Mary’s library

8,000,000
5,500,000
5,000,000
Quiz 1

We need to relocate all references to Mary’s library in my library. What option should we give to `mmap` when we map mylibrary into our address space?

a) the MAP_SHARED option
b) the MAP_PRIVATE option
c) mmap can’t be used in this situation
Relocation Revisited

- Modify shared code to effect relocation
  - result is no longer shared!
- Separate shared code from (unshared) addresses
  - position-independent code (PIC)
  - code can be placed anywhere
  - addresses in separate private section
    » pointed to by a register
The C library (and other libraries) can be mapped into different locations in different processes’ address spaces.
Mapping printf into the Address Space

- **Printf’s text**
  - read-only
  - can it be shared?
    - yes: use MAP_SHARED

- **Printf’s data**
  - read-write
  - not shared with other processes
  - initial values come from file
  - can mmap be used?
    - MAP_SHARED wouldn’t work
      - changes made to data by one process would be seen by others
    - MAP_PRIVATE does work!
      - mapped region is initialized from file
      - changes are private

For this slide, we assume relocation is dealt with through the use of position-independent code (PIC).
Mapping printf

Process 1

printf text
- page 6
- page 7

printf data
- page 31
- page 32

Process 2

printf text
- page 3
- page 4

printf data
- page 41
- page 42

Real Memory

printf
- page 0
- page 1
- page 2
- page 3

Disk

P1's printf
- page 2
- page 3

P2's printf
- page 2

P1's printf
- page 0
To provide position-independent code on x86-64, ELF requires three data structures for each dynamic executable (i.e., the program binary loaded by `exec`) and shared object: the procedure-linkage table, the global-offset table, and the relocation table. To simplify discussion, we refer to dynamic executables and shared objects as modules. The procedure linkage table contains the code that’s actually called when control is to be transferred to an externally defined routine. It is shared by all processes using the associated executable or object, and makes use of data in the global-object table to link the caller to the called program. Each process has its own private copy of each global-object table. It contains the relocated addresses of all externally defined symbols. Finally, the relocation table contains much information about each module. What is used for linking is relocation information and the symbol table, as we explain in the next few slides.

How things work is similar for other architectures, but definitely not the same.
To establish position-independent references to global variables, the compiler produces, for each module, a *global-offset table*. Modules refer to global variables indirectly by looking up their addresses in the table, using PC-relative addressing. The item needed is at some fixed offset from the beginning of the table. When the module is loaded into memory, ld-linux.so is responsible for putting into it the actual addresses of all the needed global variables.
Procedures in Shared Objects

- Lots of them
- Many are never used
- Fix up linkages on demand
Dealing with references to external procedures is considerably more complicated than dealing with references to external data. This slide shows the procedure linkage table, global offset table, and relocation information for a module that contains references to external procedures `name1` and `name2`. Let’s follow a call to procedure `name1`. The general idea is before the first call to `name1`, the actual address of the `name1` procedure is not recorded in the global-offset table. Instead, the first call to `name1` actually invokes `ld-linux.so`, which is passed parameters indicating what is really wanted. It then finds `name1` and updates the global-offset table so that things are more direct on subsequent calls.

To make this happen, references from the module to `name1` are statically linked to entry `.PLT1` in the procedure-linkage table. This entry contains an unconditional jump (via PC-relative addressing) to the address contained in the `name1` offset of the global-offset table. Initially this address is of the instruction following the jump instruction, which contains code that pushes onto the stack the offset of the `name1` entry in the relocation table. The next instruction is an unconditional jump to the beginning of the procedure-linkage table, entry `.PLT0`. Here there’s code that pushes onto the stack the second 32-bit word of the global-offset table, which contains a value identifying this module. The following instruction is an unconditional jump to the address in the third word of the global-offset table, which is conveniently the address of `ld-linux.so`. Thus control finally passes to `ld-linux.so`, which looks back on the stack and determines which module has called it and what that module really wants to call. It figures this out based on the module-identification word and the relocation table entry, which contains the offset of the `name1` entry in the global-offset table (which is what must be updated) and the index of `name1` in the symbol table (so it knows the name of what it must locate).
Finally, ld-linux.so writes the actual address of the name1 procedure into the name1 entry of the global-offset table, and, after unwinding the stack a bit, passes control to name1. On subsequent calls by the module to name1, since the global-offset table now contains name1’s address, control goes to it more directly, without an invocation of ld-linux.so.