Building and Using Shared Libraries on Linux

Shared Libraries: The Dynamic Linker

Michael Kerrisk, man7.org © 2020

mtk@man7.org

February 2020

Outline

4 The Dynamic Linker 4-1
4.1 Rpath: specifying library search paths in an object 4-3
4.2 Finding shared libraries at run time 4-11
4.3 Symbol resolution, library load order, and link maps 4-15
4.4 Debugging the operation of the dynamic linker 4-25

Outline

4 The Dynamic Linker 4-1
4.1 Rpath: specifying library search paths in an object 4-3
4.2 Finding shared libraries at run time 4-11
4.3 Symbol resolution, library load order, and link maps 4-15
4.4 Debugging the operation of the dynamic linker 4-25

Specifying library search paths in an object

- So far, we have two methods of informing the dynamic linker (DL) of location of a shared library:
  - `LD_LIBRARY_PATH`
  - Installing library in one of the standard directories
- Third method: during static linking, we can **insert a list of directories into the executable**
  - So-called "run-time library path (**rpath**) list"
  - At run time, DL will search listed directories to resolve dynamic dependencies
  - Useful if libraries will reside in locations that are fixed, but not in standard list

[TLPI §41.10]

Defining an rpath list when linking

- To embed an rpath list in an executable, use the *-rpath* linker option (*gcc -Wl,-rpath,path-to-lib-dir*)
  - Multiple *-rpath* options can be specified ⇒ ordered list
  - Alternatively, multiple directories can be specified as a colon-separated list in a single *-rpath* option
- Example:

```
$ cc -g -Wall -Wl,-rpath,$PWD -o prog prog.c \
        libdemo.so
$ objdump -p prog | grep 'R[UN]*PATH'
  RPATH                /home/mtk/tlpi/code/shlibs
$ ./prog
Called mod1-x1
Called mod2-x2
```

  - Embeds current working directory in rpath list
  - *objdump* command allows us to inspect rpath list
  - Executable now “tells” DL where to find shared library

Shared libraries can have rpath lists

- Shared libraries can themselves have dependencies
  - ⇒ can use *-rpath* linker option to embed rpath lists when building shared libraries

An rpath improvement: DT_RUNPATH

There are **two types of rpath list**:

- Differ in precedence relative to `LD_LIBRARY_PATH`
- Original (and default) rpath list has higher precedence
  - `DT_RPATH` ELF entry
- The original rpath behavior was a **design error**
  - We want user to have full control when using `LD_LIBRARY_PATH`

An rpath improvement: DT_RUNPATH

- **Newer rpath type has lower precedence**
  - Gives user possibility to override rpath at runtime using `LD_LIBRARY_PATH` **(usually what we want)**
  - `DT_RUNPATH` ELF entry
    - Supported in DL since 1999
  - Use: *cc -Wl,-rpath,some-dir-path -Wl,--enable-new-dtags*
    - *binutils* 2.24 (2013) and later: inserts only `DT_RUNPATH` entry
    - Before *binutils* 2.24, inserted `DT_RUNPATH` **and** `DT_RPATH` (to allow for old DLs that didn't understand `DT_RUNPATH`)
- If both types of rpath list are embedded in an object, **`DT_RUNPATH` has precedence**
  - I.e., DL ignores `DT_RPATH` list

“Magic” names in rpath lists

- DL understands certain special names in rpath list
  - Written as `$NAME` or `${NAME}`
- `$ORIGIN`: expands to directory containing program or library
  - Write turn-key applications!
  - Installer unpacks tarball containing application with library in (say) a subdirectory; application can be linked with:

```
cc -Wl,-rpath,'$ORIGIN/lib'
```

    - ⚠ ⚠ Note use of quotes to prevent interpretation of `$` by shell!

“Magic” names in rpath lists

- `$LIB`: expands to `lib` or `lib64`, depending on architecture
  - E.g., useful on multi-arch platforms to supply 32-bit or 64-bit library, as appropriate
- `$PLATFORM`: expands to string corresponding to processor type (e.g., `x86_64`)
  - Rpath entry can include arch-specific directory component
- DL also understands these names in some other contexts
  - `LD_LIBRARY_PATH`, `LD_PRELOAD`, & `LD_AUDIT`; see *ld.so(8)*

Outline

4 The Dynamic Linker 4-1
4.1 Rpath: specifying library search paths in an object 4-3
4.2 Finding shared libraries at run time 4-11
4.3 Symbol resolution, library load order, and link maps 4-15
4.4 Debugging the operation of the dynamic linker 4-25

Finding shared libraries at run time

When resolving dependencies in dynamic dependency list, DL deals with each dependency string as follows:

- If the string contains a slash ⇒ interpret dependency as a relative or absolute pathname
- Otherwise, search for shared library using these rules
  1. If object has `DT_RPATH` list and does **not** have `DT_RUNPATH` list, search directories in `DT_RPATH` list
  2. If `LD_LIBRARY_PATH` defined, search directories it specifies
     - For security reasons, `LD_LIBRARY_PATH` is ignored in "secure" mode (set-UID and set-GID programs, etc.)
  3. If object has `DT_RUNPATH` list, search directories in that list
  4. Check `/etc/ld.so.cache` for a corresponding entry
  5. Search `/lib` and `/usr/lib` (in that order)
     - Or `/lib64` and `/usr/lib64`

[TLPI §41.11]

Exercises

1. The directory `shlibs/mysleep` contains two files:
   - `mysleep.c`: implements a function, *mysleep(nsecs)*, which prints a message and calls *sleep()* to sleep for *nsecs* seconds.
   - `mysleep_main.c`: takes one argument that is an integer string. The program calls *mysleep()* with the numeric value specified in the command-line argument.

   Using these files, perform the following steps to create a shared library and executable in the same directory:
   - Build a shared library from `mysleep.c`.
   - Compile and link `mysleep_main.c` against the shared library to produce an executable that embeds an rpath list with the run-time location of the shared library (specified as an absolute path, e.g., use the value of *$PWD*).
   - Verify that you can successfully run the executable without the use of `LD_LIBRARY_PATH`.
     [Exercise continues on following slide]

Exercises

   - Try moving both the executable and the shared library to a different directory. What now happens when you try to run the executable? Why?

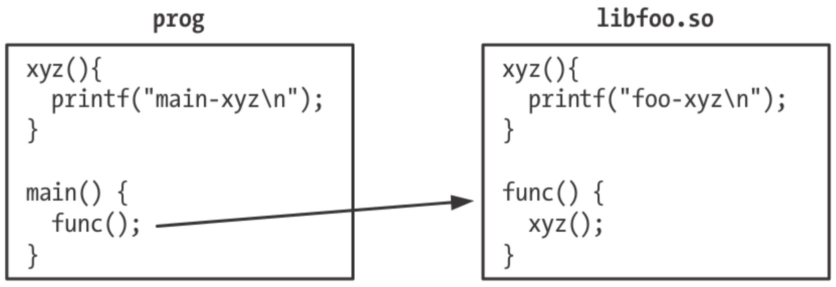
2. Now employ an rpath list that uses the `$ORIGIN` string:
   - Modify the previous example so that you create an executable with an rpath list containing the string `$ORIGIN/sub`.
     ⚠ Remember to use single quotes around `$ORIGIN`!
   - Copy the executable to some directory, and copy the shared library to a subdirectory, `sub`, under that directory. Verify that the program runs successfully.
   - If you move both the executable and the directory `sub` (which still contains the shared library) to a different location, is it still possible to run the executable?

Outline

4 The Dynamic Linker 4-1
4.1 Rpath: specifying library search paths in an object 4-3
4.2 Finding shared libraries at run time 4-11
4.3 Symbol resolution, library load order, and link maps 4-15
4.4 Debugging the operation of the dynamic linker 4-25

Run-time symbol resolution

- Suppose main program and shared library both define a function *xyz()*, and another function inside library calls *xyz()*



```
xyz(){
  printf("main-xyz\n");
}

main() {
  func();
}
```

```
xyz(){
  printf("foo-xyz\n");
}

func() {
  xyz();
}
```

- To which symbol does reference to *xyz()* resolve?
- The results may seem a little surprising:

```
$ cc -g -c -fPIC -Wall foo.c
$ cc -g -shared -o libfoo.so foo.o
$ cc -g -o prog prog.c libfoo.so
$ LD_LIBRARY_PATH=. ./prog
main-xyz
```

  - Definition in main program overrides version in library!

Maintaining historical semantics

- Surprising, but good historical reason for this behavior
- Shared libraries are designed to mirror traditional static library semantics:
  - Definition of global symbol in main program overrides version in library
  - Global symbol appears in multiple libraries?
    - ⇒ reference is resolved to first definition when **scanning libraries in left-to-right order as specified in static link command line**
- Makes transition from static to shared libraries easy

Maintaining historical semantics can cause complications

- But, default symbol resolution semantics **conflict with model of shared library as a self-contained subsystem**
  - Shared library can't guarantee that reference to its own global symbols will bind to those symbols at run time
  - Properties of shared library may change when it is aggregated into larger system
- Can be desirable to force references to global symbols within a shared library to resolve to library's own symbols

Forcing global symbol references to resolve inside library

- *-Bsymbolic* linker option causes references to global symbols within shared library to resolve to library's own symbols

```
$ cc -g -c -fPIC -Wall foo.c
$ cc -g -shared -Wl,-Bsymbolic -o libfoo.so foo.o
$ cc -g -o prog prog.c libfoo.so
$ LD_LIBRARY_PATH=. ./prog
foo-xyz
```

  - ELF `DT_SYMBOLIC` tag
- ⚠ Affects **all** symbols in shared library!
  - Other techniques can obtain this behavior on a per-symbol basis
    - (Described later)

Symbol resolution and library load order

```
         .......main_prog.......
        /         |             \
libx1.so       liby1.so          libz1.so
   |              | abc(){...}      |  call abc()
   |              |                 |
libx2.so       liby2.so          libz2.so
  abc(){...}     xyz(){...}         |
  xyz(){...}                     libz3.so
                                   xyz(){...}
```

- Main program has three dynamic dependencies
- Some libraries on which main has dependencies in turn have dependencies
  - **Note**: main program has no direct dependencies other than `libx1.so`, `liby1.so`, and `libz1.so`
    - Likewise, `libz1.so` has no direct dependency on `libz3.so`

Symbol resolution and library load order

```
          .......main_prog.......
        /          |              \
libx1.so       liby1.so          libz1.so
   |              | abc(){...}      |  call abc()
   |              |                 |
libx2.so       liby2.so          libz2.so
  abc(){...}     xyz(){...}         |
  xyz(){...}                     libz3.so
                                   xyz(){...}
```

- libx2.so and liby1.so both define public function *abc()*
- When *abc()* is called from inside libz1.so, which instance of *abc()* is invoked?
- Call to *abc()* resolves to definition in liby1.so

Symbol resolution and library load order

```
          .......main_prog.......
        /          |              \
libx1.so       liby1.so          libz1.so
   |              | abc(){...}      |  call abc()
   |              |                 |
libx2.so       liby2.so          libz2.so
  abc(){...}     xyz(){...}         |
  xyz(){...}                     libz3.so
                                   xyz(){...}
```

- Dependent libraries are added in **breadth-first order**
  - Immediate dependencies of main program are loaded first
  - Then dependencies of those dependencies, and so on
    - Libraries that are already loaded are skipped (but are reference counted)
- Symbols are resolved by searching libraries in load order

Symbol resolution and library load order

```
          .......main_prog.......
        /          |              \
libx1.so       liby1.so         libz1.so
   |               |  abc(){...}    |   call abc()
   |               |                |   call xyz()
libx2.so       liby2.so         libz2.so
  abc(){...}     xyz(){...}         |
  xyz(){...}                    libz3.so
                                  xyz(){...}
```

- A quiz...
- libx2.so, liby2.so, and libz3.so all define public function *xyz()*
- When *xyz()* is called from inside libz1.so, which instance of *xyz()* is invoked?
- Call to *xyz()* resolves to definition in libx2.so

Link-map lists ("namespaces")

- Set of shared objects that have been loaded by application is recorded on a **link-map list** (AKA "namespace")
  - Doubly linked list that is arranged in library load order
  - See definition of struct link_map in <link.h>
  - *dl_iterate_phdr(3)* can be used to iterate through link map
    - (Manual page has an example program)
  - See also *dlinfo(3)*, which obtains info about a dynamically loaded object

Outline

4 The Dynamic Linker 4-1
4.1 Rpath: specifying library search paths in an object 4-3
4.2 Finding shared libraries at run time 4-11
4.3 Symbol resolution, library load order, and link maps 4-15
4.4 Debugging the operation of the dynamic linker 4-25

The LD_DEBUG environment variable

- LD_DEBUG can be used to monitor operation of dynamic linker
  - LD_DEBUG="*value*" prog
  - To list LD_DEBUG options, without executing program:

```
$ LD_DEBUG=help ./prog
Valid options for the LD_DEBUG environment variable are:

  libs         display library search paths
  reloc        display relocation processing
  files        display progress for input file
  symbols      display symbol table processing
  bindings     display information about symbol binding
  versions     display version dependencies
  scopes       display scope information
  all          all previous options combined
  statistics   display relocation statistics
  unused       determined unused DSOs
  help         display this help message and exit

To direct the debugging output into a file instead of
standard output a filename can be specified using the
LD_DEBUG_OUTPUT environment variable.
```

  - TLPI §42.6

Exercises

The files in the directory `shlibs/sym_res_load_order` set up the scenario shown earlier under the heading *Symbol resolution and library load order* (slide 4-23). The `main` program uses *dl_iterate_phdr()* to display the link-map order of the loaded shared objects.

1. Inspect the source code used to build the various shared libraries.
2. Use *make(1)* to build the shared libraries and the main program, and use the following command to run the program in order to verify the link-map order and also to see which versions of *abc()* and *xyz()* are called from inside `libz1.so`:

   ```
   LD_LIBRARY_PATH=. ./main
   ```

3. Run the program using `LD_DEBUG=libs` and use the dynamic linker's debug output to verify the order in which the shared libraries are loaded.
4. Run the program using `LD_DEBUG=symbols` and use the dynamic linker's debug output to discover which definitions the calls to *abc()* and *xyz()* bind to.

Notes