ELF1 7 Examples - 3 Object File main.o - ELF Study 1999

Young W. Lim

2020-01-18 Sat

Outline

1. Based on
2. Sumary of the relocaton results for `rel.o` object file
   - TOC
   - 1. Reloc summary for `main.o` object file reloc
   - 2. Symbols and sections for `main.o` object file
3. Compiling for `main.o` object file
   - Symbol references in the definition of `main`
   - Compiling for `.text` section of `main`
4. Locating relocs of `main.o` object file
   - TOC
   - Locating `.text` section relocs of `main.o` executable file

Based on

"Study of ELF loading and relocs", 1999
http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

Compling 32-bit program on 64-bit gcc

- gcc -v
- gcc -m32 t.c
- sudo apt-get install gcc-multilib
- sudo apt-get install g++-multilib
- gcc-multilib
- g++-multilib
- gcc -m32
- objdump -m i386

TOC: Summary of the results

- `rel.o` object file relocs
- `main.o` object file relocs

TOC: 1. Reloc summary for `main.o` object file

- Relocation table sections for `main.o` object file
- Relocation listing sections for `main.o` object file
- a) text section relocs of an object file `main.o`
- b) `.rel.text` reloc listing of an object file `main.o`

Relocation table sections for main.o object files

- for main.o

	-fno-pic	default	-fPIC
.plt			
.plt.got			
.got			
.got.plt			

```
readelf -t run-fno-pic | grep -e .plt -e .got -e .rel
```

Relocation listing sections for main.o object files

- for main.o

	-fno-pic	default	-fPIC
.rel.data			
.rel.data.rel			
.rel.text	✓	✓	✓
.rel.dyn			
.rel.plt			
.rel.got			

```
readelf -t run-fno-pic | grep -e .plt -e .got -e .rel
```

a) text section relocs of an object file main.o

- text section relocs of main.o file
  - global data symbol reference (cPub)
    R_386_GOT32 in .text : when GOT is used (default, -fPIC)
    R_386_32 in .text : otherwise (-fno-pic)
  - global function symbol reference (fPub)
    R_386_PLT32 in .text : when PLT is used (default, -fPIC)
    R_386_PC32 in .text : otherwise (-fno-pic)

b) .rel.text reloc listing of an object file main.o

- .rel.text relocs of main.o file

	-fno-pic	default	-fPIC
cPub	R_386_32 in .text	R_386_GOT32x in .text	R_386_GOT32x in .text
fPub	R_386_PC32 in .text	R_386_PLT32 in .text	R_386_PLT32 in .text

- fPub is defined in other module (rel.o)

TOC: Symbols and sections for `main.o` object file

- Symbol table in `main.o` (-fno-pic, default, -fPIC)
- Section header in `main.o` (-fno-pic, default, -fPIC)
- Relocs in `main.o` (-fno-pic, default, -fPIC)

Symbol table in main.o (-fno-pic)

```
young@USys2:~$ readelf -s main-fno-pic.o

Symbol table '.symtab' contains 11 entries:
   Num:    Valor  Tam  Tipo    Unión  Vis      Nombre Ind
     0: 00000000    0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00000000    0 FILE    LOCAL  DEFAULT  ABS main.c
     8: 00000000   47 FUNC    GLOBAL DEFAULT    1 main
     9: 00000000    0 NOTYPE  GLOBAL DEFAULT  UND fPub
    10: 00000000    0 NOTYPE  GLOBAL DEFAULT  UND cPub
```

https://stackoverflow.com/questions/1685483/how-can-i-examine-contents-of-a-data-s

Symbol table in main.o (default)

```
young@USys2:~$ readelf -s main-default.o

Symbol table '.symtab' contains 15 entries:
   Num:    Valor  Tam  Tipo    Unión  Vis      Nombre Ind
     0: 00000000    0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00000000    0 FILE    LOCAL  DEFAULT  ABS main.c
    10: 00000000   61 FUNC    GLOBAL DEFAULT    2 main
    12: 00000000    0 NOTYPE  GLOBAL DEFAULT  UND _GLOBAL_OFFSET_TABLE_
    13: 00000000    0 NOTYPE  GLOBAL DEFAULT  UND fPub
    14: 00000000    0 NOTYPE  GLOBAL DEFAULT  UND cPub
```

https://stackoverflow.com/questions/1685483/how-can-i-examine-contents-of-a-data-s

Symbol table in main.o (-fPIC)

```
young@USys2:~$ readelf -s main-fPIC.o

Symbol table '.symtab' contains 15 entries:
   Num:    Valor  Tam  Tipo    Unión  Vis      Nombre Ind
     0: 00000000    0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00000000    0 FILE    LOCAL  DEFAULT  ABS main.c
    10: 00000000   61 FUNC    GLOBAL DEFAULT    2 main
    12: 00000000    0 NOTYPE  GLOBAL DEFAULT  UND _GLOBAL_OFFSET_TABLE_
    13: 00000000    0 NOTYPE  GLOBAL DEFAULT  UND fPub
    14: 00000000    0 NOTYPE  GLOBAL DEFAULT  UND cPub
```

https://stackoverflow.com/questions/1685483/how-can-i-examine-contents-of-a-data-s

Section header in main.o (-fno-pic)

```
young@USys2:~$ readelf -S main-fno-pic.o

  [Nr] Nombre              Tipo            Direc    Desp   Tam    ES Opt En Inf Al
  [ 1] .text               PROGBITS        00000000 000034 00002f 00  AX  0   0  1
  [ 2] .rel.text           REL             00000000 00019c 000010 08   I  9   1  4
  [ 3] .data               PROGBITS        00000000 000063 000000 00  WA  0   0  1
  [ 4] .bss                NOBITS          00000000 000063 000000 00  WA  0   0  1
  [ 9] .symtab             SYMTAB          00000000 0000d4 0000b0 10     10   8  4
```

Section header in main.o (default)

```
young@USys2:~$ readelf -S main-default.o
```

[Nr]	Nombre	Tipo	Direc	Desp	Tam	ES	Opt	En	Inf	Al
[2]	.text	PROGBITS	00000000	00003c	00003d	00	AX	0	0	1
[3]	.rel.text	REL	00000000	000240	000020	08	I	11	2	4
[4]	.data	PROGBITS	00000000	000079	000000	00	WA	0	0	1
[5]	.bss	NOBITS	00000000	000079	000000	00	WA	0	0	1
[11]	.symtab	SYMTAB	00000000	00010c	0000f0	10		12	10	4

Section header in main.o (-fPIC)

```
young@USys2:~$ readelf -S main-fPIC.o

  [Nr] Nombre              Tipo            Direc    Desp   Tam    ES Opt En Inf Al
  [ 2] .text               PROGBITS        00000000 00003c 00003d 00  AX  0   0  1
  [ 3] .rel.text           REL             00000000 000240 000020 08   I 11   2  4
  [ 4] .data               PROGBITS        00000000 000079 000000 00  WA  0   0  1
  [ 5] .bss                NOBITS          00000000 000079 000000 00  WA  0   0  1
  [11] .symtab             SYMTAB          00000000 00010c 0000f0 10     12  10  4
```

Relocs of main.o (-fno-pic)

```
young@USys2:~$ readelf -r main-fno-pic.o

La sección de reubicación '.rel.text' at offset 0x19c contains 2 entries:
 Desplaz    Info    Tipo            Val.Símbolo Nom. Símbolo
00000017  00000902 R_386_PC32        00000000   fPub
00000021  00000a01 R_386_32          00000000   cPub
```

Relocs of main.o (default)

```
young@USys2:~$ readelf -r main-default.o

La sección de reubicación '.rel.text' at offset 0x240 contains 4 entries:
 Desplaz    Info    Tipo            Val.Símbolo Nom. Símbolo
00000016  00000c0a R_386_GOTPC       00000000   _GLOBAL_OFFSET_TABLE_
00000020  00000d04 R_386_PLT32       00000000   fPub
0000002b  00000e2b R_386_GOT32X      00000000   cPub
```

Relocs of main.o (-fPIC)

```
young@USys2:~$ readelf -r main-fPIC.o

La sección de reubicación '.rel.text' at offset 0x240 contains 4 entries:
 Desplaz    Info    Tipo            Val.Símbolo Nom. Símbolo
00000016  00000c0a R_386_GOTPC       00000000   _GLOBAL_OFFSET_TABLE_
00000020  00000d04 R_386_PLT32       00000000   fPub
0000002b  00000e2b R_386_GOT32X      00000000   cPub
```

relocs for fPub(123) - global function symbol referefence

- when the executable is created,
  the R_386_PC32 at fPub(123)
  will have an PLT entry location of the shared library
- call to the PLT entry will be performed first
- the GOT entry in the shared library
  will get a R_386_JUMP_SLOT reloc
  using fPub symbol

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

relocs for cPub : global data symbol reference (1)

- the data reference of cPub will cause a local copy
  of the global cPub to be created in the data space of the app
- the data reference of cPub is changed
  to point to this new global data, and
  the reloc is resolved
- this new global gets a R_386_COPY reloc,
  using the symbol cPub

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

relocs for cPub : global symbol reference (2)

- the cPub symbol has the following characteristics
  - the symbol references data
  - the symbol is 1 byte long
- at run time, the dynamic linker will
  find the symbol cPub in one of the *libraries* and
  copy the 1 byte down from the library into the app data space
- the dynamic linker will then publish this new address
  as the address of cPub

`http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html`

TOC: Locating relocs of `main.o` object file

- Locating `.text` section relocs of `main.o` executable file

TOC: Locating .text section relocs of main.o executable file

- (a) call fPub in the .text section of main.o
- (b) call fPub in the .text section of run_dynamic
- (c) referencing cPub in the .text section of main.o
- (c) referencing cPub in the .text section of run_dynamic
- Relocs to be converted in the .text section of run_dynamic

(a) calling fPub in the .text section of main.o

- main.o with -fno-pic

```
16:   e8 fc ff ff ff          call   17 <main+0x17> ; call function at 17
                      17: R_386_PC32  fPub
                                ;   17 = 0 + 17 ; fPub func ref location
                                ;   -4 = fffffffc ; offset (pc adjust)
                                ;   00000000 <main>: ...
```

- main.o with default (fPub : PLT)

```
1f:   e8 fc ff ff ff          call   20 <main+0x20> ; call function at 20
                      20: R_386_PLT32 fPub
                                ;   20 = 0 + 20 ; fPub func ref location
                                ;   -4 = fffffffc ; offset (pc adjust)
                                ;   00000000 <main>: ...
```

- main.o with -fPIC (fPub : PLT)

```
1f:   e8 fc ff ff ff          call   20 <main+0x20> ; call function at 20
                      20: R_386_PLT32 fPub
                                ;   20 = 0 + 20 ; fPub func ref loation
                                ;   -4 = fffffffc ; offset (pc adjust)
                                ;   00000000 <main>: ...
```

(b) calling fPub in the .text section of run-dynamic

- run-dynamic with -fno-pic

```
613:  e8 fc ff ff ff          call   614 <main+0x17> ; call func at 614
                      614: R_386_PC32 fPub
                                ;   614 = 5fd + 17 ; fPub func ref location
                                ;   -4 = fffffffc; offset
                                ;   000005fd <main>: ...
```

- run_dynamic with default (fPub : PLT)

```
5fc:  e8 7f fe ff ff          call   480 <fPub@plt> ; call func at 480
                      5fd: R_386_PLT32        fPub
                                ;   5fd = fPub func ref location
                                ;  -181 = fffffe7f offset (5fd+4-181=480)
                                ;   00000480 <fPub@plt>:
                                ;   000005dd <main>: ...
```

- run_dynamic with -fPIC (fPub : PLT)

```
5fc:  e8 7f fe ff ff          call   480 <fPub@plt> ; call func at 480
                      5fd: R_386_PLT32        fPub
                                ;   5fd = fPub func ref location
                                ;  -181 = fffffe7f offset (5fd+4-181=480)
                                ;   00000480 <fPub@plt>:
                                ;   000005dd <main>: ...
```

gcc -Wl,-q is used

(c) referencing cPub in the .text section of main.o

- main.o with -fno-pic

```
20:   a1 00 00 00 00          mov    0x0,%eax
                    21: R_386_32    cPub
                                ;   21 = cPub symbol ref location
                                ;    0 = offset (no pc adjust)
```

- main.o with default (cPub : GOT)

```
29:   8b 83 00 00 00 00       mov    0x0(%ebx),%eax
                    2b: R_386_GOT32X        cPub
                                ;   2b = cPub symbol ref location
                                ;    0 = offset (no pc adjust)
```

- main.o with -fPIC (cPub : GOT)

```
29:   8b 83 00 00 00 00       mov    0x0(%ebx),%eax
                    2b: R_386_GOT32X        cPub
                                ;   2b = cPub symbol ref location
                                ;    0 = offset (no pc adjust)
```

(d) referencing cPub in the .text section of run-dynamic

- run-dynamic with -fno-pic

```
61d:  a1 00 00 00 00          mov    0x0,%eax
                      61e: R_386_32   cPub
                                    ; 61e = cPub symbol ref location
                                    ;   0 = offset (no pc adjust)
```

- run_dynamic with default (cPub : GOT)

```
606:  8b 83 24 00 00 00       mov    0x24(%ebx),%eax
                      608: R_386_GOT32X       cPub  ... -Wl,-q
                                    ; 608 = cPub symbol ref location
                                    ;  24 = offset (1fd4+24 = 1ff8)
                                    ; 00001fd4 <_GLOBAL_OFFSET_TABLE_>: ...
                                    ; 00001fd4 <.got>: ...
```

- run_dynamic with -fPIC (cPub : GOT)

```
606:  8b 83 24 00 00 00       mov    0x24(%ebx),%eax
                      608: R_386_GOT32X       cPub ... -Wl,-q
                                    ; 608 = cPub symbol ref location
                                    ;  24 = offset (1fd4 +24 = 1ff8)
                                    ; 00001fd4 <_GLOBAL_OFFSET_TABLE_>: ...
                                    ; 00001fd4 <.got>: ...
```

gcc -Wl,-q is used

Relocs to be converted in the .text section of run-dynamic

- .text section relocs of main.o with -fno-pic

```
cPUb in .text (R_386_PC)     >>>>  cPUb in .text (R_386_PC)
                                   cPub in .bss  (R_386_COPY)
```

- .text section relocs of main.o with default

```
fPub in .text (R_386_PLT32)  >>>>  slot  in .got.plt (R_386_JUMP_SLOT)
cPUb in .text (R_386_GOT32)  >>>>  entry in .got     (R_386_GLOB_DAT)
```

- .text section relocs of main.o with -fPIC (fPub : PLT)

```
fPub in .text (R_386_PLT32)  >>>>  slot  in .got.plt (R_386_JUMP_SLOT)
cPUb in .text (R_386_GOT32)  >>>>  entry in .got     (R_386_GLOB_DAT)
```