ELF1 7 Examples - 8 Relocs Listings - ELF Study 1999

Young W. Lim

2020-01-21 Tue

Outline

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
- -Wl,-q

TOC: Relocs background in shared object and executable files

- Relocs in a PIC shared object (.so) file
- Relocs in a non-PIC executable file
- PIC, PIE, and non-PIC executables

Example library code

```
typedef struct {
  char* p;
  char (*f)(int);
} _st;

char fPub(int a) {
  return a;
}

static char fLocal(int b) {
  return b;
}

char cPub;              // uninitialized
static char cLocal;     // uninitialized
```

```
_st a[] = { { &cLocal,  // 1
              fLocal }, // 2
            { &cPub,    // 3
              fPub } }; // 4

int foo(int a) {        // 5
  return fPub(a)        // 6
       + fLocal(a)      // 7
       + (int) &cPub    // 8
       + cPub           // 9
       + (int) &cLocal  // 10
       + cLocal;        // 11
}
```

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

Example executable code

- the main function code

```
extern int fPub(int);
extern int cPub;

int main() {
  return fPub(123)   // 1
       + cPub;       // 2
}
```

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

Using a shared library

- creating a shared library

```
gcc -m32 -fPIC -c -g rel.c
gcc -m32 -shared rel.o -o librel.so
```

- linking with a shared library

```
gcc -m32 -c -g main.c
gcc -m32 main.o -Wl,-q -L/home/young/ -lrel -o run_dynamic
```

- run a dynamic executable

```
LD_LIBRARY_PATH=/home/young/ ./run_dynamic
```

https://renenyffenegger.ch/notes/development/languages/C-C-plus-plus/GCC/create-libraries/index

.rel.text, rel.o, -fno-pic (1/1)

```
Relocation section '.rel.text' at offset 0x254 contains 5 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000018  00000a02 R_386_PC32        00000000   fPub
00000033  00000b01 R_386_32          00000001   cPub
0000003c  00000b01 R_386_32          00000001   cPub
00000046  00000401 R_386_32          00000000   .bss
0000004f  00000401 R_386_32          00000000   .bss
```

.rel.data, rel.o, -fno-pic (1/1)

```
Relocation section '.rel.data' at offset 0x27c contains 4 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000000  00000401 R_386_32          00000000   .bss
00000004  00000201 R_386_32          00000000   .text
00000008  00000b01 R_386_32          00000001   cPub
0000000c  00000a01 R_386_32          00000000   fPub
```

.rel.dyn, librel.so, -fno-pic (1/1)

```
Relocation section '.rel.dyn' at offset 0x2e8 contains 16 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
000004f3  00000008 R_386_RELATIVE
000004fc  00000008 R_386_RELATIVE
00001f30  00000008 R_386_RELATIVE
00001f34  00000008 R_386_RELATIVE
0000200c  00000008 R_386_RELATIVE
00002010  00000008 R_386_RELATIVE
00002014  00000008 R_386_RELATIVE
000004c5  00000902 R_386_PC32        000004ad   fPub
0000201c  00000901 R_386_32          000004ad   fPub
000004e0  00000a01 R_386_32          00002022   cPub
000004e9  00000a01 R_386_32          00002022   cPub
00002018  00000a01 R_386_32          00002022   cPub
00001ff0  00000106 R_386_GLOB_DAT    00000000   __cxa_finalize
00001ff4  00000206 R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
00001ff8  00000306 R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
00001ffc  00000406 R_386_GLOB_DAT    00000000   __gmon_start__
```

.rel.text, main.o, -fno-pic (1/1)

```
Relocation section '.rel.text' at offset 0x19c contains 2 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000017  00000902 R_386_PC32        00000000   fPub
00000021  00000a01 R_386_32          00000000   cPub
```

.rel.dyn, run_dynamic, -fno-pic (1/1)

```
Relocation section '.rel.dyn' at offset 0x3e8 contains 11 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00001ec8  00000008 R_386_RELATIVE
00001ecc  00000008 R_386_RELATIVE
00001ff8  00000008 R_386_RELATIVE
00002004  00000008 R_386_RELATIVE
00000614  00000602 R_386_PC32        00000000   fPub
0000061e  00000b01 R_386_32          00002008   cPub
00001fec  00000106 R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
00001ff0  00000206 R_386_GLOB_DAT    00000000   __cxa_finalize@GLIBC_2.1.3
00001ff4  00000306 R_386_GLOB_DAT    00000000   __gmon_start__
00001ffc  00000506 R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
00002008  00000b05 R_386_COPY        00002008   cPub
```

.rel.plt, run_dynamic, -fno-pic (1/1)

```
Relocation section '.rel.plt' at offset 0x440 contains 2 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00001fe4  00000407 R_386_JUMP_SLOT   00000000   __libc_start_main@GLIBC_2.0
00001fe8  00000607 R_386_JUMP_SLOT   00000000   fPub
```

.rel.text, rel.o, default (1/1)

```
Relocation section '.rel.text' at offset 0x37c contains 11 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000004  00001002 R_386_PC32        00000000   __x86.get_pc_thunk.ax
00000009  0000110a R_386_GOTPC       00000000   _GLOBAL_OFFSET_TABLE_
00000016  00001002 R_386_PC32        00000000   __x86.get_pc_thunk.ax
0000001b  0000110a R_386_GOTPC       00000000   _GLOBAL_OFFSET_TABLE_
0000002a  00001502 R_386_PC32        00000000   __x86.get_pc_thunk.bx
00000030  0000110a R_386_GOTPC       00000000   _GLOBAL_OFFSET_TABLE_
00000038  00000f02 R_386_PC32        00000000   fPub
00000055  0000122b R_386_GOT32X      00000001   cPub
0000005d  0000122b R_386_GOT32X      00000001   cPub
0000006b  00000409 R_386_GOTOFF      00000000   .bss
00000074  00000409 R_386_GOTOFF      00000000   .bss
```

.rel.data.rel, rel.o, default (1/1)

```
Relocation section '.rel.data.rel' at offset 0x3d4 contains 4 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000000  00000401 R_386_32          00000000   .bss
00000004  00000201 R_386_32          00000000   .text
00000008  00001201 R_386_32          00000001   cPub
0000000c  00000f01 R_386_32          00000000   fPub
```

.rel.dyn, librel.so, default (1/1)

```
Relocation section '.rel.dyn' at offset 0x2e8 contains 13 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00001f2c  00000008 R_386_RELATIVE
00001f30  00000008 R_386_RELATIVE
0000200c  00000008 R_386_RELATIVE
00002010  00000008 R_386_RELATIVE
00002014  00000008 R_386_RELATIVE
000004d5  00000902 R_386_PC32        0000049d   fPub
0000201c  00000901 R_386_32          0000049d   fPub
00001fec  00000106 R_386_GLOB_DAT    00000000   __cxa_finalize
00001ff0  00000206 R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
00001ff4  00000a06 R_386_GLOB_DAT    00002022   cPub
00002018  00000a01 R_386_32          00002022   cPub
00001ff8  00000306 R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
00001ffc  00000406 R_386_GLOB_DAT    00000000   __gmon_start__
```

.rel.text, main.o, default (1/1)

```
Relocation section '.rel.text' at offset 0x240 contains 4 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000010  00000b02 R_386_PC32        00000000   __x86.get_pc_thunk.bx
00000016  00000c0a R_386_GOTPC       00000000   _GLOBAL_OFFSET_TABLE_
00000020  00000d04 R_386_PLT32       00000000   fPub
0000002b  00000e2b R_386_GOT32X      00000000   cPub
```

.rel.dyn, run_dynamic, default (1/1)

```
Relocation section '.rel.dyn' at offset 0x3e4 contains 9 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00001ecc  00000008 R_386_RELATIVE
00001ed0  00000008 R_386_RELATIVE
00001ff4  00000008 R_386_RELATIVE
00002004  00000008 R_386_RELATIVE
00001fe8  00000106 R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
00001fec  00000206 R_386_GLOB_DAT    00000000   __cxa_finalize@GLIBC_2.1.3
00001ff0  00000306 R_386_GLOB_DAT    00000000   __gmon_start__
00001ff8  00000506 R_386_GLOB_DAT    00000000   cPub
00001ffc  00000606 R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
```

.rel.plt, run_dynamic, default (1/1)

```
Relocation section '.rel.plt' at offset 0x42c contains 2 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00001fe0  00000407 R_386_JUMP_SLOT   00000000   __libc_start_main@GLIBC_2.0
00001fe4  00000707 R_386_JUMP_SLOT   00000000   fPub
```

.rel.text, rel.o, -fPIC (1/1)

```
Relocation section '.rel.text' at offset 0x384 contains 11 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000004  00001002 R_386_PC32        00000000   __x86.get_pc_thunk.ax
00000009  0000110a R_386_GOTPC       00000000   _GLOBAL_OFFSET_TABLE_
00000016  00001002 R_386_PC32        00000000   __x86.get_pc_thunk.ax
0000001b  0000110a R_386_GOTPC       00000000   _GLOBAL_OFFSET_TABLE_
0000002a  00001502 R_386_PC32        00000000   __x86.get_pc_thunk.bx
00000030  0000110a R_386_GOTPC       00000000   _GLOBAL_OFFSET_TABLE_
0000003b  00000f04 R_386_PLT32       00000000   fPub
0000005b  0000122b R_386_GOT32X      00000001   cPub
00000063  0000122b R_386_GOT32X      00000001   cPub
00000071  00000409 R_386_GOTOFF      00000000   .bss
0000007a  00000409 R_386_GOTOFF      00000000   .bss
```

.rel.data.rel, rel.o, -fPIC (1/1)

```
Relocation section '.rel.data.rel' at offset 0x3dc contains 4 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000000  00000401 R_386_32          00000000   .bss
00000004  00000201 R_386_32          00000000   .text
00000008  00001201 R_386_32          00000001   cPub
0000000c  00000f01 R_386_32          00000000   fPub
```

.rel.dyn, librel.so, -fPIC (1/1)

```
Relocation section '.rel.dyn' at offset 0x2e8 contains 12 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00001f24  00000008 R_386_RELATIVE
00001f28  00000008 R_386_RELATIVE
00002010  00000008 R_386_RELATIVE
00002014  00000008 R_386_RELATIVE
00002018  00000008 R_386_RELATIVE
00001fec  00000106 R_386_GLOB_DAT    00000000   __cxa_finalize
00001ff0  00000206 R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
00001ff4  00000a06 R_386_GLOB_DAT    00002026   cPub
0000201c  00000a01 R_386_32          00002026   cPub
00001ff8  00000306 R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
00001ffc  00000406 R_386_GLOB_DAT    00000000   __gmon_start__
00002020  00000901 R_386_32          000004ad   fPub
```

.rel.plt, librel.so, -fPIC (1/1)

```
Relocation section '.rel.plt' at offset 0x348 contains 1 entry:
 Offset     Info    Type            Sym.Value  Sym. Name
0000200c  00000907 R_386_JUMP_SLOT   000004ad   fPub
```

.rel.text, main.o, -fPIC (1/1)

```
Relocation section '.rel.text' at offset 0x240 contains 4 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000010  00000b02 R_386_PC32        00000000   __x86.get_pc_thunk.bx
00000016  00000c0a R_386_GOTPC       00000000   _GLOBAL_OFFSET_TABLE_
00000020  00000d04 R_386_PLT32       00000000   fPub
0000002b  00000e2b R_386_GOT32X      00000000   cPub
```

.rel.dyn, run_dynamic, -fPIC (1/1)

```
Relocation section '.rel.dyn' at offset 0x3e4 contains 9 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00001ecc  00000008 R_386_RELATIVE
00001ed0  00000008 R_386_RELATIVE
00001ff4  00000008 R_386_RELATIVE
00002004  00000008 R_386_RELATIVE
00001fe8  00000106 R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
00001fec  00000206 R_386_GLOB_DAT    00000000   __cxa_finalize@GLIBC_2.1.3
00001ff0  00000306 R_386_GLOB_DAT    00000000   __gmon_start__
00001ff8  00000506 R_386_GLOB_DAT    00000000   cPub
00001ffc  00000606 R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
```

.rel.plt, run_dynamic, -fPIC (1/1)

```
Relocation section '.rel.plt' at offset 0x42c contains 2 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00001fe0  00000407 R_386_JUMP_SLOT   00000000   __libc_start_main@GLIBC_2.0
00001fe4  00000707 R_386_JUMP_SLOT   00000000   fPub
```