Zad. 6

niedziela, 14 maja 2023 21:00

Zadanie 6. Jądro systemu `Linux` nie potrafi załadować do pamięci pliku wykonywalnego skonsolidowanego dynamicznie – musi o to poprosić **interpreter programu** [2, 5]. Rozważmy plik wykonywalny «`/bin/sleep`». Na podstawie zawartości jego sekcji «`.interp`» podaj ścieżkę do **konsolidatora dynamicznego** [2, 5]. Przy pomocy polecenia «`nm`» wyświetl wszystkie *symbole dynamiczne* – `ld.so(8)` będzie musiał musiał znaleźć ich definicje w bibliotekach dynamicznych. Przy pomocy polecenie «`readelf -d`» wyświetl sekcję «`.dynamic`» [2, 5-9] i wskaż biblioteki, w których będą wyszukiwane definicje symboli. Na podstawie podręcznika `ldconfig(8)` znajdź plik konfiguracyjny przechowujący ścieżki, gdzie konsolidator będzie szukał bibliotek. Wskaż skąd zostanie załadowana biblioteka «`libc.so.6`». Przy pomocy polecenia `ldd(1)` wyświetl pod jakie adresy konsolidator załadowałby biblioteki, gdyby miał załadować program do pamięci. Czemu za każdym razem adresy bibliotek są inne?

```
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$ file /bin/sleep
/bin/sleep: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/
ld-linux-x86-64.so.2, BuildID[sha1]=9605b84bc84dab0a28a772dcebed48b0b98ec3a9, for GNU/Linux 3.2.0, stripped
```

> In computer science, an **interpreter** is a computer program that directly executes instructions written in a programming or scripting language, without requiring them previously to have been compiled into a machine language program. An interpreter generally uses one of the following strategies for program execution:

```
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$ objdump -s -j .interp /bin/sleep

/bin/sleep:     file format elf64-x86-64

Contents of section .interp:
 0318 2f6c6962 36342f6c 642d6c69 6e75782d  /lib64/ld-linux-
 0328 7838362d 36342e73 6f2e3200           x86-64.so.2.
```

ścieżka

> In computing, a **dynamic linker** is the part of an operating system that loads and links the shared libraries needed by an executable when it is executed (at "run time"), by copying the content of libraries from persistent storage to RAM, filling jump tables and relocating pointers. The specific operating system and executable format determine how the dynamic linker functions and how it is implemented.
>
> Linking is often referred to as a process that is performed when the executable is compiled, while a dynamic linker is a special part of an operating system that loads external shared libraries into a running process and then binds those shared libraries dynamically to the running process. This approach is also called **dynamic linking** or **late linking**.

```
mluczynski@mluczynski:~/Desktop/studia/ask/Lista 9/lista_9$ nm -D /bin/sleep
```

dużo

```
Dynamic section at offset 0x7c60 contains 23 entries:
  Tag        Type                         Name/Value
 0x0000000000000001 (NEEDED)             Shared library: [libc.so.6]
 0x000000000000000c (INIT)               0x2000
 0x000000000000000d (FINI)               0x5174
 0x000000006ffffef5 (GNU_HASH)           0x3b0
 0x0000000000000005 (STRTAB)             0x960
 0x0000000000000006 (SYMTAB)             0x3d8
 0x000000000000000a (STRSZ)              702 (bytes)
 0x000000000000000b (SYMENT)             24 (bytes)
 0x0000000000000015 (DEBUG)              0x0
 0x0000000000000003 (PLTGOT)             0x8e10
 0x0000000000000002 (PLTRELSZ)           1080 (bytes)
 0x0000000000000014 (PLTREL)             RELA
 0x0000000000000017 (JMPREL)             0xe78
 0x0000000000000007 (RELA)               0xcf8
 0x0000000000000008 (RELASZ)             384 (bytes)
 0x0000000000000009 (RELAENT)            24 (bytes)
 0x000000000000001e (FLAGS)              BIND_NOW
 0x000000006ffffffb (FLAGS_1)            Flags: NOW PIE
 0x000000006ffffffe (VERNEED)            0xc98
 0x000000006fffffff (VERNEEDNUM)         1
 0x000000006ffffff0 (VERSYM)             0xc1e
 0x000000006ffffff9 (RELACOUNT)          5
 0x0000000000000000 (NULL)               0x0
```

When the dynamic linker creates the memory segments for an object file, the dependencies (recorded in DT_NEEDED entries of the dynamic structure) tell what shared objects are needed to supply the program's services. By repeatedly connecting referenced shared objects and their dependencies, the dynamic linker builds a complete process image. When resolving symbolic references, the dynamic linker examines the symbol tables with a breadth-first search. That is, it first looks at the symbol table of the executable program itself, then at the symbol tables of the DT_NEEDED entries (in order), and then at the second level DT_NEEDED entries, and so on. Shared object files must be readable by the process; other permissions are not required.

ldconfig creates the necessary links and cache to the most recent shared libraries found in the directories specified on the command line, in the file */etc/ld.so.conf*, and in the trusted directories, */lib* and */usr/lib* (on some 64-bit architectures such as x86-64, */lib* and */usr/lib* are the trusted directories for 32-bit libraries, while */lib64* and */usr/lib64* are used for 64-bit libraries).

```
mluczynski@mluczynski:/etc/ld.so.conf.d$ ls
fakeroot-x86_64-linux-gnu.conf  libc.conf             zz_i386-biarch-compat.conf
i386-linux-gnu.conf             x86_64-linux-gnu.conf
mluczynski@mluczynski:/etc/ld.so.conf.d$ cat libc.conf
# libc default configuration
/usr/local/lib
mluczynski@mluczynski:/etc/ld.so.conf.d$
```

```
mluczynski@mluczynski:/lib/x86_64-linux-gnu$ ls | grep libc.so
libc.so
libc.so.6
mluczynski@mluczynski:/lib/x86_64-linux-gnu$
```

sława zaladuje

```
mluczynski@mluczynski:/lib/x86_64-linux-gnu$ ldd /bin/sleep
        linux-vdso.so.1 (0x00007ffd801d4000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f2e99e00000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f2e9a20d000)
mluczynski@mluczynski:/lib/x86_64-linux-gnu$
```

```
mluczynski@mluczynski:/lib/x86_64-linux-gnu$ ldd /bin/sleep
        linux-vdso.so.1 (0x00007ffce63fc000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f14fd000000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f14fd393000)
mluczynski@mluczynski:/lib/x86_64-linux-gnu$
```

```
mluczynski@mluczynski:/lib/x86_64-linux-gnu$ ldd /bin/sleep
        linux-vdso.so.1 (0x00007ffce63fc000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f14fd000000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f14fd393000)
mluczynski@mluczynski:/lib/x86_64-linux-gnu$
```