Robert Brodin - Operating Systems A 2020 - Professor Wills
Project Two - Part Three

1. Observation of program execution behaviors shows that many system calls are invoked as part of starting up a program. To examine this start-up behavior, construct a simple program that makes no system calls and analyze it using traceanal. Do all programs exhibit a similar start-up behavior in terms of which system calls are used and their relative sequence?

I created a program with no system calls, that simply printed out “Where is my mind…” (my respect if you know the song), and ran the strace script on it and analyzed the system call dump file compared to the strace dump file from running the “ls” command. What I found was that both of them shared a lot of the same system calls in the creation of the program. The sequence is similar up until the system call “mprotect”.

My custom command	Ls command
execve("./customcommand", ["./customcommand"], 0x7fffffffe160 /* 48 vars */) = 0 1. brk(NULL) = 0x555555756000 2. access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory) 3. access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory) 4. openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3 5. fstat(3, {st_mode=S_IFREG|0644, st_size=95608, ...}) = 0 6. mmap(NULL, 95608, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7ffff7fdf000 7. close(3) = 0 8. access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory) 9. openat(AT_FDCWD, "/usr/lib/x86_64-linux-gnu/libstdc++.so.6", O_RDONLY|O_CLOEXEC) = 3 10. read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\220\304\10\0\0\0\0\0"..., 832) = 832 11. fstat(3, {st_mode=S_IFREG|0644, st_size=1594864, ...}) = 0 12. mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7ffff7fdd000 13. mmap(NULL, 3702848, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7ffff7a4c000	execve("/bin/ls", ["ls", "-l"], 0x7fffffffe158 /* 48 vars */) = 0 1. brk(NULL) = 0x555555776000 2. access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory) 3. access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory) 4. openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3 5. fstat(3, {st_mode=S_IFREG|0644, st_size=95608, ...}) = 0 6. mmap(NULL, 95608, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7ffff7fdf000 7. close(3) = 0 8. access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory) 9. openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libselinux.so.1", O_RDONLY|O_CLOEXEC) = 3 10. read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\20b\0\0\0\0\0\0"..., 832) = 832 11. fstat(3, {st_mode=S_IFREG|0644, st_size=154832, ...}) = 0 12. mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7ffff7fdd000 13. mmap(NULL, 2259152, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7ffff7bad000

```
   14.
mprotect(0x7ffff7bc5000, 2097152, PROT_NONE) =
0
   15.
mmap(0x7ffff7dc5000, 49152,
PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3,
0x179000) = 0x7ffff7dc5000
   16.
mmap(0x7ffff7dd1000, 12352,
PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) =
0x7ffff7dd1000
   17.
close(3)                                = 0
   18.
access("/etc/ld.so.nohwcap", F_OK)      = -1
ENOENT (No such file or directory)
   19.
openat(AT_FDCWD,
"/lib/x86_64-linux-gnu/libc.so.6",
O_RDONLY|O_CLOEXEC) = 3
   20.
read(3,
"\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\
0\260\34\2\0\0\0\0\0"..., 832) = 832
   21.
fstat(3, {st_mode=S_IFREG|0755,
st_size=2030544, ...}) = 0
   22.
mmap(NULL, 4131552, PROT_READ|PROT_EXEC,
MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7ffff765b000
   23.
mprotect(0x7ffff7842000, 2097152, PROT_NONE) =
0
   24.
mmap(0x7ffff7a42000, 24576,
PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3,
0x1e7000) = 0x7ffff7a42000
   25.
mmap(0x7ffff7a48000, 15072,
PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) =
0x7ffff7a48000
   26.
close(3)                                = 0
   27.
access("/etc/ld.so.nohwcap", F_OK)      = -1
ENOENT (No such file or directory)
   28.
openat(AT_FDCWD,
"/lib/x86_64-linux-gnu/libm.so.6",
O_RDONLY|O_CLOEXEC) = 3
   29.
read(3,
"\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\
0\200\272\0\0\0\0\0\0"..., 832) = 832
   30.
fstat(3, {st_mode=S_IFREG|0644,
st_size=1700792, ...}) = 0
   31.
mmap(NULL, 3789144, PROT_READ|PROT_EXEC,
MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7ffff72bd000
   32.
mprotect(0x7ffff745a000, 2093056, PROT_NONE) =
0
   33.
```

```
   14.
mprotect(0x7ffff7bd2000, 2093056, PROT_NONE) =
0
   15.
mmap(0x7ffff7dd1000, 8192,
PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3,
0x24000) = 0x7ffff7dd1000
   16.
mmap(0x7ffff7dd3000, 6352,
PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) =
0x7ffff7dd3000
   17.
close(3)                                = 0
   18.
access("/etc/ld.so.nohwcap", F_OK)      = -1
ENOENT (No such file or directory)
   19.
openat(AT_FDCWD,
"/lib/x86_64-linux-gnu/libc.so.6",
O_RDONLY|O_CLOEXEC) = 3
   20.
read(3,
"\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\
0\260\34\2\0\0\0\0\0"..., 832) = 832
   21.
fstat(3, {st_mode=S_IFREG|0755,
st_size=2030544, ...}) = 0
   22.
mmap(NULL, 4131552, PROT_READ|PROT_EXEC,
MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7ffff77bc000
   23.
mprotect(0x7ffff79a3000, 2097152, PROT_NONE) =
0
   24.
mmap(0x7ffff7ba3000, 24576,
PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3,
0x1e7000) = 0x7ffff7ba3000
   25.
mmap(0x7ffff7ba9000, 15072,
PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) =
0x7ffff7ba9000
   26.
close(3)                                = 0
   27.
access("/etc/ld.so.nohwcap", F_OK)      = -1
ENOENT (No such file or directory)
   28.
openat(AT_FDCWD,
"/lib/x86_64-linux-gnu/libpcre.so.3",
O_RDONLY|O_CLOEXEC) = 3
   29.
read(3,
"\177ELF\2\1\1\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\
0 \25\0\0\0\0\0\0"..., 832) = 832
   30.
fstat(3, {st_mode=S_IFREG|0644,
st_size=464824, ...}) = 0
   31.
mmap(NULL, 2560264, PROT_READ|PROT_EXEC,
MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7ffff754a000
   32.
mprotect(0x7ffff75ba000, 2097152, PROT_NONE) =
0
   33.
```

```
mmap(0x7ffff7659000, 8192,
PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3,
0x19c000) = 0x7ffff7659000
   34.
close(3)                                = 0
   35.
access("/etc/ld.so.nohwcap", F_OK)      = -1
ENOENT (No such file or directory)
   36.
openat(AT_FDCWD,
"/lib/x86_64-linux-gnu/libgcc_s.so.1",
O_RDONLY|O_CLOEXEC) = 3
   37.
read(3,
"\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\
0\300*\0\0\0\0\0\0"..., 832) = 832
   38.
fstat(3, {st_mode=S_IFREG|0644, st_size=96616,
...}) = 0
   39.
mmap(NULL, 2192432, PROT_READ|PROT_EXEC,
MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7ffff70a5000
   40.
mprotect(0x7ffff70bc000, 2093056, PROT_NONE) =
0
   41.
mmap(0x7ffff72bb000, 8192,
PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3,
0x16000) = 0x7ffff72bb000
   42.
close(3)                                = 0
   43.
mmap(NULL, 8192, PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7ffff7fdb000
   44.
arch_prctl(ARCH_SET_FS, 0x7ffff7fdbd00) = 0
   45.
mprotect(0x7ffff7a42000, 16384, PROT_READ) = 0

   46.
mprotect(0x7ffff72bb000, 4096, PROT_READ) = 0
   47.
mprotect(0x7ffff7659000, 4096, PROT_READ) = 0
   48.
mmap(NULL, 8192, PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7ffff7fd9000
   49.
mprotect(0x7ffff7dc5000, 40960, PROT_READ) = 0

   50.
mprotect(0x555555754000, 4096, PROT_READ) = 0
   51.
   52. mprotect(0x7ffff7ffc000, 4096,
       PROT_READ) = 0
```

```
mmap(0x7ffff77ba000, 8192,
PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3,
0x70000) = 0x7ffff77ba000
   34.
close(3)                                = 0
   35.
access("/etc/ld.so.nohwcap", F_OK)      = -1
ENOENT (No such file or directory)
   36.
openat(AT_FDCWD,
"/lib/x86_64-linux-gnu/libdl.so.2",
O_RDONLY|O_CLOEXEC) = 3
   37.
read(3,
"\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\
0P\16\0\0\0\0\0\0"..., 832) = 832
   38.
fstat(3, {st_mode=S_IFREG|0644, st_size=14560,
...}) = 0
   39.
mmap(NULL, 2109712, PROT_READ|PROT_EXEC,
MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7ffff7346000
   40.
mprotect(0x7ffff7349000, 2093056, PROT_NONE) =
0
   41.
mmap(0x7ffff7548000, 8192,
PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3,
0x2000) = 0x7ffff7548000
   42.
close(3)                                = 0
   43.
access("/etc/ld.so.nohwcap", F_OK)      = -1
ENOENT (No such file or directory)
   44.
openat(AT_FDCWD,
"/lib/x86_64-linux-gnu/libpthread.so.0",
O_RDONLY|O_CLOEXEC) = 3
   45.
read(3,
"\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\
0000b\0\0\0\0\0\0"..., 832) = 832
   46.
fstat(3, {st_mode=S_IFREG|0755,
st_size=144976, ...}) = 0
   47.
mmap(NULL, 2221184, PROT_READ|PROT_EXEC,
MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7ffff7127000
   48.
mprotect(0x7ffff7141000, 2093056, PROT_NONE) =
0
```

2. Researchers have proposed using the system call sequence of a program as a “signature” for that program as a means to detect if a copy of a program is substituted by an intruder. Investigate the validity of this idea by checking if the signature of different executions of the same program are the same. The particular counts of system calls may vary, but are the sequences similar? What if different command line arguments are used for a command? Is there variation in the sequence? Does the sequence change if the amount of data or duration

of execution varies for a program?

Investigating different executions of the same program, the system call sequences are nearly identical, with the only difference being the arguments in the specific system calls. Different command line arguments shift the amount of system calls used for a command because sometimes different arguments invoke different parts of a program. The sequence does not change very much of the duration of execution varies.

3. How much variation and commonality do you observe from invocations of different commands? You should try to separate out the start-up behavior common to all commands and the command-specific portion.

There is a lot of variation with the order of commands (ignoring the start-up behavior), but there are a lot of the same system calls used, just in a different order. I would compare it to building a building, many architects could design a building using one type of brick as the foundation, and then concrete on another part and then maybe steel beams on another. Another architect could use those same three building materials in a completely different way and have a building that looks nothing like the other building. The same “materials” or system calls are there, but the order and location makes all of the difference.