Donghyun Park

Prof. Hakner

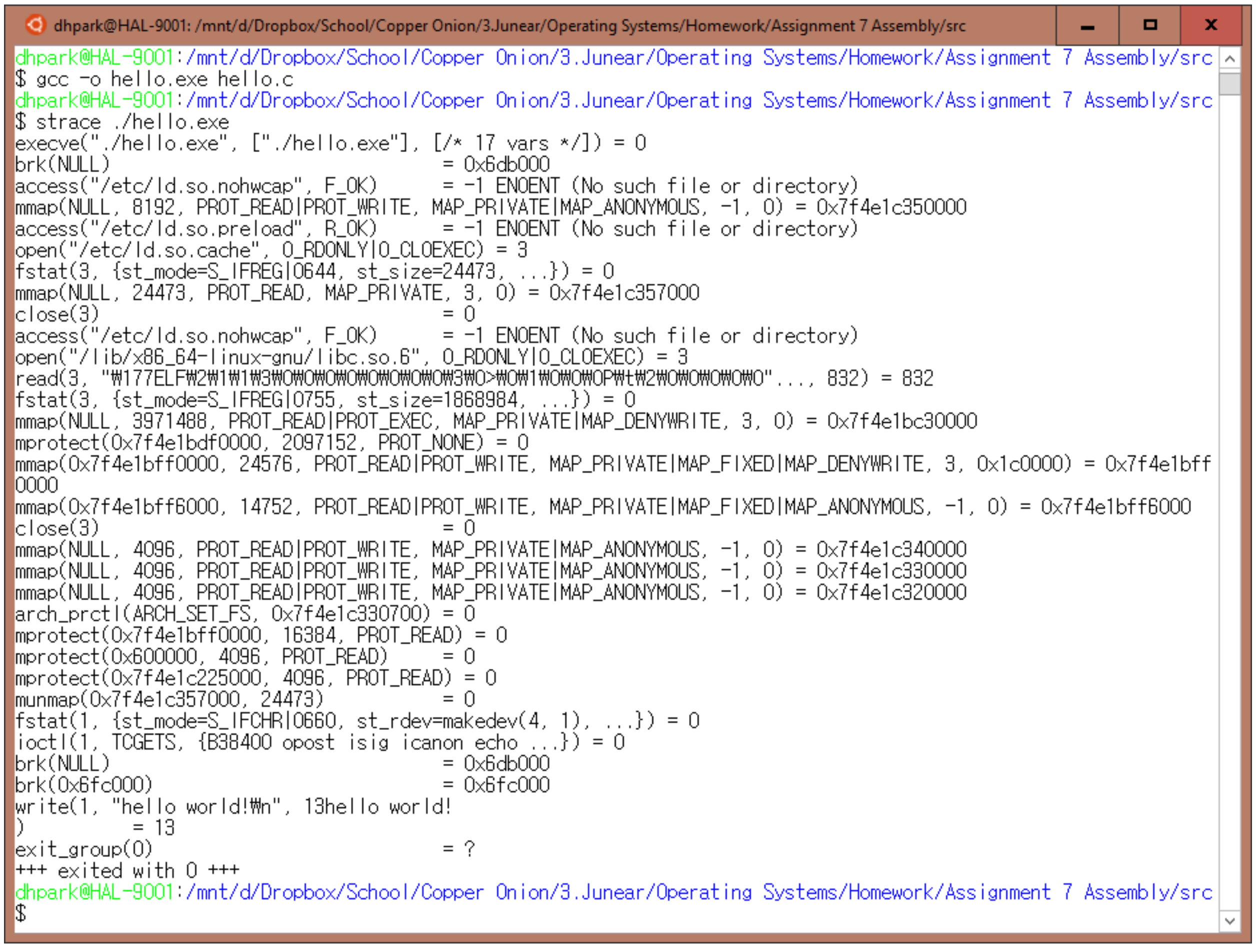
Operating Systems

12/27/17

PSet 7 – Strace and Assembly

Problem 1 – using strace

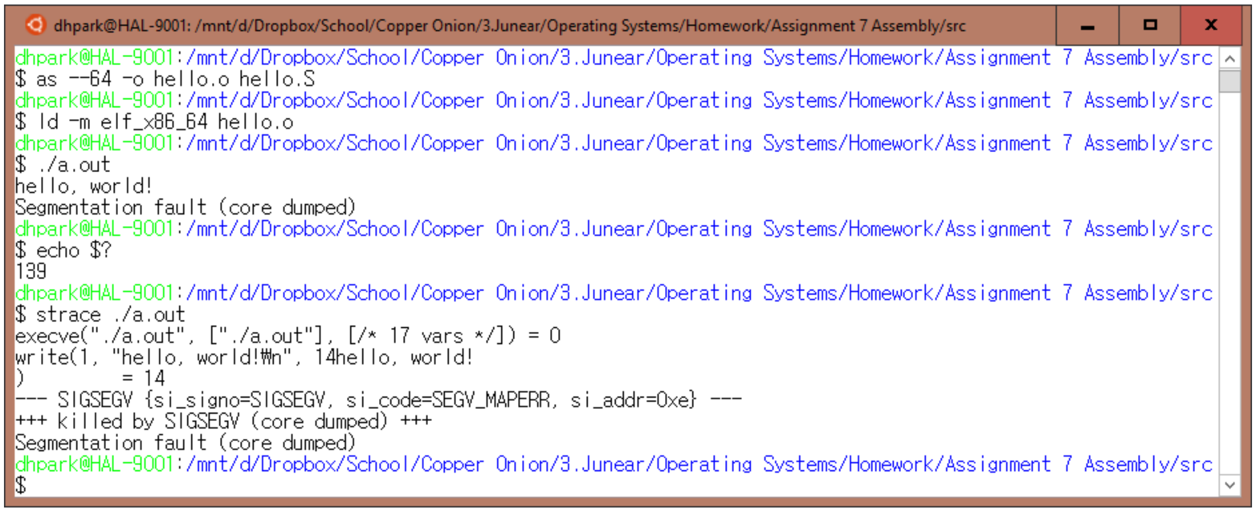
Not sure why, might be a windows locale thingy, but all \ symbols print out to be the Korean currency symbol ₩ for some reason.


dhpark@HAL-9001: /mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src

```
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ gcc -o hello.exe hello.c
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ strace ./hello.exe
execve("./hello.exe", ["./hello.exe"], [/* 17 vars */]) = 0
brk(NULL)                               = 0x6db000
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e1c350000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=24473, ...}) = 0
mmap(NULL, 24473, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f4e1c357000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "₩177ELF₩2₩1₩1₩3₩0₩0₩0₩0₩0₩0₩0₩0₩3₩0>₩0₩1₩0₩0₩0P₩t₩2₩0₩0₩0₩0₩0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=1868984, ...}) = 0
mmap(NULL, 3971488, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f4e1bc30000
mprotect(0x7f4e1bdf0000, 2097152, PROT_NONE) = 0
mmap(0x7f4e1bff0000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x1c0000) = 0x7f4e1bff
0000
mmap(0x7f4e1bff6000, 14752, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x7f4e1bff6000
close(3)                                = 0
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e1c340000
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e1c330000
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e1c320000
arch_prctl(ARCH_SET_FS, 0x7f4e1c330700) = 0
mprotect(0x7f4e1bff0000, 16384, PROT_READ) = 0
mprotect(0x600000, 4096, PROT_READ)     = 0
mprotect(0x7f4e1c225000, 4096, PROT_READ) = 0
munmap(0x7f4e1c357000, 24473)           = 0
fstat(1, {st_mode=S_IFCHR|0660, st_rdev=makedev(4, 1), ...}) = 0
ioctl(1, TCGETS, {B38400 opost isig icanon echo ...}) = 0
brk(NULL)                               = 0x6db000
brk(0x6fc000)                           = 0x6fc000
write(1, "hello world!₩n", 13hello world!
)         = 13
exit_group(0)                           = ?
+++ exited with 0 +++
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$
```

Problem 2 – pure assembly

```
.text
.global _start

_start:
  mov $1,%rax      #write system call
  mov $1,%rdi      #output to fd 1(stdout)
  mov $msg,%rsi    #msg to output
  mov $14,%rdx     #legnth of msg
  syscall
  .data

msg:
  .ascii "hello, world!\n"
```

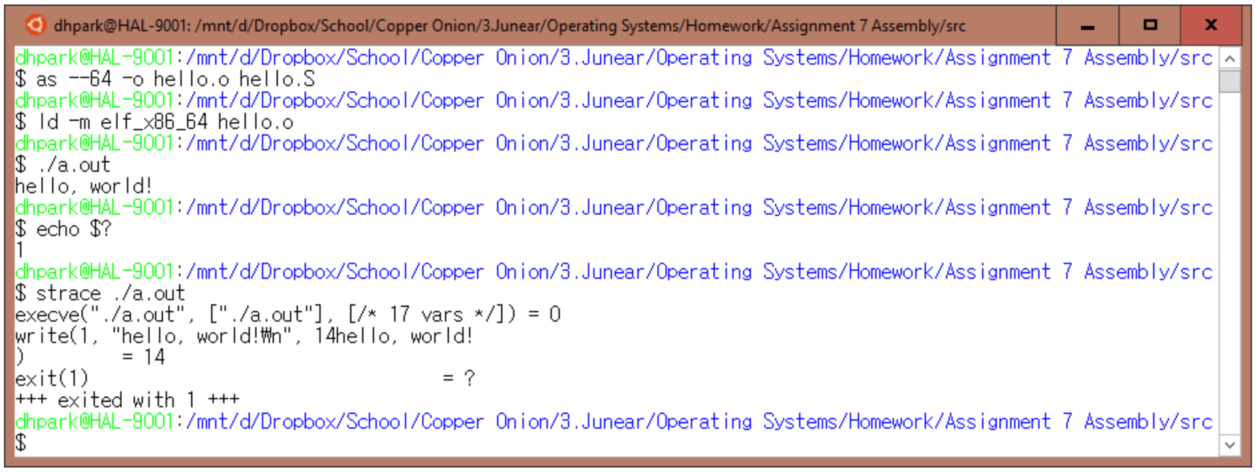

dhpark@HAL-9001: /mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src

```
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ as --64 -o hello.o hello.S
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ ld -m elf_x86_64 hello.o
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ ./a.out
hello, world!
Segmentation fault (core dumped)
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ echo $?
139
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ strace ./a.out
execve("./a.out", ["./a.out"], [/* 17 vars */]) = 0
write(1, "hello, world!₩n", 14hello, world!
)          = 14
--- SIGSEGV {si_signo=SIGSEGV, si_code=SEGV_MAPERR, si_addr=0xe} ---
+++ killed by SIGSEGV (core dumped) +++
Segmentation fault (core dumped)
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$
```

Problem 3 – exit code

After the write system call, the program terminates with the exit value 139 as seen by the echo $?, and the signal was SIGSEGV as seen by the strace. This makes sense because SIGSEGV is value 11, and the UNIX convention follows that the errno value of 128 added to 11 results in 139. The reason behind this error is due to the fact that the %rax register is volatile and thus not available at the program's termination.

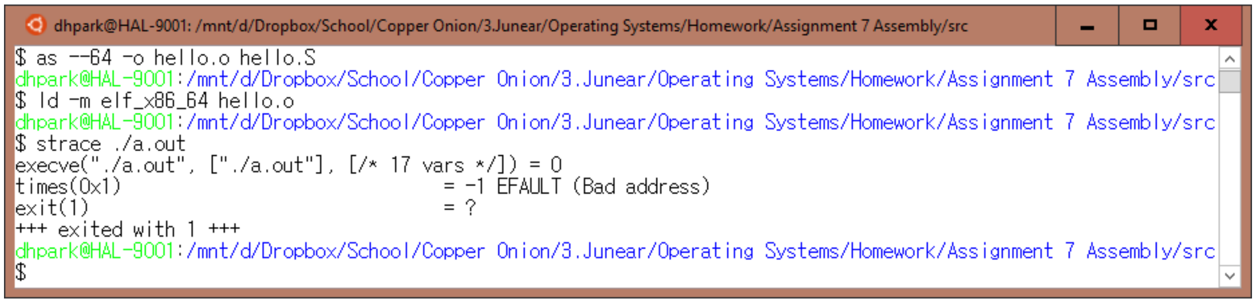
```
.text
.global _start

_start:
  mov $1,%rax      #write system call
  mov $1,%rdi      #output to fd 1(stdout)
  mov $msg,%rsi    #msg to output
  mov $14,%rdx     #legnth of msg
  syscall
  mov $1,%rdi       #return code for exit syscall
  mov $60,%rax      #exit system call
  syscall
  .data

msg:
  .ascii "hello, world!\n"
```



```
dhpark@HAL-9001: /mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ as --64 -o hello.o hello.S
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ ld -m elf_x86_64 hello.o
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ ./a.out
hello, world!
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ echo $?
1
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ strace ./a.out
execve("./a.out", ["./a.out"], [/* 17 vars */]) = 0
write(1, "hello, world!₩n", 14hello, world!
)        = 14
exit(1)                                 = ?
+++ exited with 1 +++
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$
```

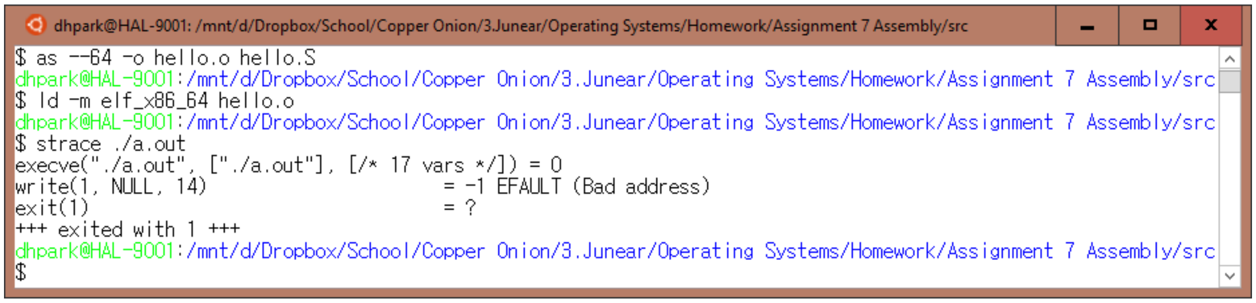
Problem 4 – system call validation

1. Replaced write system call value with 100



```
dhpark@HAL-9001: /mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ as --64 -o hello.o hello.S
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ ld -m elf_x86_64 hello.o
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ strace ./a.out
execve("./a.out", ["./a.out"], [/* 17 vars */]) = 0
times(0x1)                              = -1 EFAULT (Bad address)
exit(1)                                 = ?
+++ exited with 1 +++
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$
```

2. Passed invalid address for write string



```
dhpark@HAL-9001: /mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ as --64 -o hello.o hello.S
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ ld -m elf_x86_64 hello.o
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$ strace ./a.out
execve("./a.out", ["./a.out"], [/* 17 vars */]) = 0
write(1, NULL, 14)                      = -1 EFAULT (Bad address)
exit(1)                                 = ?
+++ exited with 1 +++
dhpark@HAL-9001:/mnt/d/Dropbox/School/Copper Onion/3.Junear/Operating Systems/Homework/Assignment 7 Assembly/src
$
```