Siddhant Shah
COMS 4187
11/20/2018

1. The CVE-2018-2698 entry deals with the VRAM allocated to the virtual machine for graphics processing. The interface between the host and guest VM is handled by the VGA device that is created with the shared memory. This is the same interface that allows mouse pointer integration, and splitting the virtualbox window across multiple monitors.

By using VDMA commands, specifically the transfer command, memory can be copied outside the bounds of the VRAM memory and into the host OS. This is allowed to happen due to a lack of bounds checks.

Oracle has issued a patch that can be obtained by updating VirtualBox.

2. Apache suExec allows the user to run CGIscripts as a different user. The permissions of that common user account can be adjusted for security. This is useful as it allows users on a site to call scripts without giving them permissions directly. This prevents malicious attackers from sending a request while a privilege escalated script is running. Apache's suExec also conveniently logs to a single file, so it can be easily viewed when multiple users do something that causes errors.

3. There are four protections mentioned in the reading. One of them is binary packing, where they XOR the binary with a hard coded key so that the instructions aren't visible until the key is applied, which only happens during execution. The second is by running many checksums to check for modifications to the binary. Third, they have implemented anti-debugging techniques which trap debugging threads if execution takes longer than expected. Finally, they obfuscate the code by having the binary modify itself while executing. This is all done to conceal what Skype actually does, and make it hard for people to copy and deconstruct their code.

There are drawbacks in that if breaches occur, it would take many times longer to figure out where the vulnerability is. Additionally, there's a real performance drawback to having to do all these extra operations.

4. By making the listing in the directory available, there is a rather simple way for all users to communicate. Users can simply place their messages in the names of the files that they create. Formatting it as <Sender>_<TimeStamp>_<message>, and then having the directory viewer show most recent files first, would essentially allow a chatroom of sorts.

As for dodging the system administrator, you'd set up a command that checks when the directory is updated. When it is, you create a file that says "Received" and delete it after a few seconds. Meanwhile, the sender sees the "Received" message and their script deletes their original message after your script has already copied the message to a log file. At this point, the "Received" file is deleted by you, and the original message is deleted by the sender, leaving the directory empty and you with what was sent.

Programming Exercises:

1.

siddhant@siddhant-VirtualBox:~/jail$ J=~/jail

```
siddhant@siddhant-VirtualBox:~/jail$ mkdir bin
siddhant@siddhant-VirtualBox:~/jail$ ls
bin
siddhant@siddhant-VirtualBox:~/jail$ cp -v /bin/ls $J/bin
'/bin/ls' -> '/home/siddhant/jail/bin/ls'
siddhant@siddhant-VirtualBox:~/jail$ cp -v /bin/bash $J/bin
'/bin/bash' -> '/home/siddhant/jail/bin/bash'
siddhant@siddhant-VirtualBox:~/jail$ cd bin
siddhant@siddhant-VirtualBox:~/jail/bin$ ls
bash  ls
siddhant@siddhant-VirtualBox:~/jail/bin$ cd ..
siddhant@siddhant-VirtualBox:~/jail$ ldd bin/bash
        linux-vdso.so.1 (0x00007ffc76341000)
        libtinfo.so.5 => /lib/x86_64-linux-gnu/libtinfo.so.5 (0x00007ff644ece000)
        libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007ff644cca000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007ff6448d9000)
        /lib64/ld-linux-x86-64.so.2 (0x00007ff645412000)
siddhant@siddhant-VirtualBox:~/jail$ mkdir lib
siddhant@siddhant-VirtualBox:~/jail$ mkdir lib64
siddhant@siddhant-VirtualBox:~/jail$ cp -v  /lib/x86_64-linux-gnu/libtinfo.so.5 /lib/x86_64-linux-
gnu/libdl.so.2 /lib/x86_64-linux-gnu/libc.so.6 $J/lib
'/lib/x86_64-linux-gnu/libtinfo.so.5' -> '/home/siddhant/jail/lib/libtinfo.so.5'
'/lib/x86_64-linux-gnu/libdl.so.2' -> '/home/siddhant/jail/lib/libdl.so.2'
'/lib/x86_64-linux-gnu/libc.so.6' -> '/home/siddhant/jail/lib/libc.so.6'
siddhant@siddhant-VirtualBox:~/jail$ cp -v /lib64/ld-linux-x86-64.so.2 $J/lib64
'/lib64/ld-linux-x86-64.so.2' -> '/home/siddhant/jail/lib64/ld-linux-x86-64.so.2'
siddhant@siddhant-VirtualBox:~/jail$ ls
bin  lib  lib64
siddhant@siddhant-VirtualBox:~/jail$ list="$(ldd /bin/ls | egrep -o '/lib.*\.[0-9]')"
siddhant@siddhant-VirtualBox:~/jail$ cd lib
siddhant@siddhant-VirtualBox:~/jail/lib$ ls
libc.so.6  libdl.so.2  libtinfo.so.5
siddhant@siddhant-VirtualBox:~/jail/lib$ echo $list
/lib/x86_64-linux-gnu/libselinux.so.1 /lib/x86_64-linux-gnu/libc.so.6
/lib/x86_64-linux-gnu/libpcre.so.3 /lib/x86_64-linux-gnu/libdl.so.2 /lib64/ld-linux-x86-64.so.2
/lib/x86_64-linux-gnu/libpthread.so.0
siddhant@siddhant-VirtualBox:~/jail/lib$ cp -v /lib/x86_64-linux-gnu/libselinux.so.1 /lib/x86_64-
linux-gnu/libc.so.6 /lib/x86_64-linux-gnu/libpcre.so.3 /lib/x86_64-linux-gnu/libdl.so.2 $J/lib
'/lib/x86_64-linux-gnu/libselinux.so.1' -> '/home/siddhant/jail/lib/libselinux.so.1'
'/lib/x86_64-linux-gnu/libc.so.6' -> '/home/siddhant/jail/lib/libc.so.6'
'/lib/x86_64-linux-gnu/libpcre.so.3' -> '/home/siddhant/jail/lib/libpcre.so.3'
'/lib/x86_64-linux-gnu/libdl.so.2' -> '/home/siddhant/jail/lib/libdl.so.2'
siddhant@siddhant-VirtualBox:~/jail/lib$ cp -v /lib/x86_64-linux-gnu/libpthread.so.0 $J/lib
'/lib/x86_64-linux-gnu/libpthread.so.0' -> '/home/siddhant/jail/lib/libpthread.so.0'
siddhant@siddhant-VirtualBox:~/jail/lib$ cp -v /lib64/ld-linux-x86-64.so.2 $J/lib64
'/lib64/ld-linux-x86-64.so.2' -> '/home/siddhant/jail/lib64/ld-linux-x86-64.so.2'
siddhant@siddhant-VirtualBox:~/jail/lib$ ldd /bin/ls
        linux-vdso.so.1 (0x00007fffacfac000)
        libselinux.so.1 => /lib/x86_64-linux-gnu/libselinux.so.1 (0x00007f66f1b18000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f66f1727000)
        libpcre.so.3 => /lib/x86_64-linux-gnu/libpcre.so.3 (0x00007f66f14b5000)
        libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007f66f12b1000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f66f1f62000)
        libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007f66f1092000)
```

siddhant@siddhant-VirtualBox:~/jail/lib$ sudo chroot $J /bin/bash
[sudo] password for siddhant:
bash-4.4# ls /
bin lib lib64
bash-4.4# ls /etc/
ls: cannot access '/etc/': No such file or directory
bash-4.4# HW="hello world"
bash-4.4# echo $HW > hello
bash-4.4# exit
exit
siddhant@siddhant-VirtualBox:~/jail/lib$ cd ..
siddhant@siddhant-VirtualBox:~/jail$ ls
bin hello lib lib64
siddhant@siddhant-VirtualBox:~/jail$ cat hello
hello world

2.

Output:

siddhant@siddhant-VirtualBox:/var$ strace ls
execve("/bin/ls", ["ls"], 0x7fffcf950b00 /* 51 vars */) = 0
brk(NULL)   = 0x5565a3d85000
access("/etc/ld.so.nohwcap", F_OK)   = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)   = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=86128, ...}) = 0
mmap(NULL, 86128, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f0f837ed000
close(3)   = 0
access("/etc/ld.so.nohwcap", F_OK)   = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libselinux.so.1", O_RDONLY|O_CLOEXEC) = 3
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
fstat(3, {st_mode=S_IFREG|0644, st_size=154832, ...}) = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7f0f837eb000
mmap(NULL, 2259152, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7f0f833b4000
mprotect(0x7f0f833d9000, 2093056, PROT_NONE) = 0
mmap(0x7f0f835d8000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_DENYWRITE, 3, 0x24000) = 0x7f0f835d8000
mmap(0x7f0f835da000, 6352, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_ANONYMOUS, -1, 0) = 0x7f0f835da000
close(3)   = 0
access("/etc/ld.so.nohwcap", F_OK)   = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/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\0\260\34\2\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=2030544, ...}) = 0
mmap(NULL, 4131552, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7f0f82fc3000
mprotect(0x7f0f831aa000, 2097152, PROT_NONE) = 0

```
mmap(0x7f0f833aa000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_DENYWRITE, 3, 0x1e7000) = 0x7f0f833aa000
mmap(0x7f0f833b0000, 15072, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_ANONYMOUS, -1, 0) = 0x7f0f833b0000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libpcre.so.3", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0 \25\0\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0644, st_size=464824, ...}) = 0
mmap(NULL, 2560264, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7f0f82d51000
mprotect(0x7f0f82dc1000, 2097152, PROT_NONE) = 0
mmap(0x7f0f82fc1000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_DENYWRITE, 3, 0x70000) = 0x7f0f82fc1000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libdl.so.2", O_RDONLY|O_CLOEXEC) = 3
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
fstat(3, {st_mode=S_IFREG|0644, st_size=14560, ...}) = 0
mmap(NULL, 2109712, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7f0f82b4d000
mprotect(0x7f0f82b50000, 2093056, PROT_NONE) = 0
mmap(0x7f0f82d4f000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_DENYWRITE, 3, 0x2000) = 0x7f0f82d4f000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libpthread.so.0", O_RDONLY|O_CLOEXEC) = 3
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
fstat(3, {st_mode=S_IFREG|0755, st_size=144976, ...}) = 0
mmap(NULL, 2221184, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7f0f8292e000
mprotect(0x7f0f82948000, 2093056, PROT_NONE) = 0
mmap(0x7f0f82b47000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_DENYWRITE, 3, 0x19000) = 0x7f0f82b47000
mmap(0x7f0f82b49000, 13440, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_ANONYMOUS, -1, 0) = 0x7f0f82b49000
close(3)                                = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7f0f837e9000
arch_prctl(ARCH_SET_FS, 0x7f0f837ea040) = 0
mprotect(0x7f0f833aa000, 16384, PROT_READ) = 0
mprotect(0x7f0f82b47000, 4096, PROT_READ) = 0
mprotect(0x7f0f82d4f000, 4096, PROT_READ) = 0
mprotect(0x7f0f82fc1000, 4096, PROT_READ) = 0
mprotect(0x7f0f835d8000, 4096, PROT_READ) = 0
mprotect(0x5565a3829000, 8192, PROT_READ) = 0
mprotect(0x7f0f83803000, 4096, PROT_READ) = 0
munmap(0x7f0f837ed000, 86128)           = 0
set_tid_address(0x7f0f837ea310)         = 30508
set_robust_list(0x7f0f837ea320, 24)     = 0
rt_sigaction(SIGRTMIN, {sa_handler=0x7f0f82933cb0, sa_mask=[], sa_flags=SA_RESTORER|
SA_SIGINFO, sa_restorer=0x7f0f82940890}, NULL, 8) = 0
```

```
rt_sigaction(SIGRT_1, {sa_handler=0x7f0f82933d50, sa_mask=[], sa_flags=SA_RESTORER|
SA_RESTART|SA_SIGINFO, sa_restorer=0x7f0f82940890}, NULL, 8) = 0
rt_sigprocmask(SIG_UNBLOCK, [RTMIN RT_1], NULL, 8) = 0
prlimit64(0, RLIMIT_STACK, NULL, {rlim_cur=8192*1024, rlim_max=RLIM64_INFINITY}) = 0
statfs("/sys/fs/selinux", 0x7ffc94041470) = -1 ENOENT (No such file or directory)
statfs("/selinux", 0x7ffc94041470)      = -1 ENOENT (No such file or directory)
brk(NULL)                               = 0x5565a3d85000
brk(0x5565a3da6000)                     = 0x5565a3da6000
openat(AT_FDCWD, "/proc/filesystems", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0444, st_size=0, ...}) = 0
read(3, "nodev\tsysfs\nnodev\trootfs\nnodev\tr"..., 1024) = 463
read(3, "", 1024)                       = 0
close(3)                                = 0
access("/etc/selinux/config", F_OK)     = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/usr/lib/locale/locale-archive", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=10281936, ...}) = 0
mmap(NULL, 10281936, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f0f81f5f000
close(3)                                = 0
ioctl(1, TCGETS, {B38400 opost isig icanon echo ...}) = 0
ioctl(1, TIOCGWINSZ, {ws_row=24, ws_col=80, ws_xpixel=0, ws_ypixel=0}) = 0
openat(AT_FDCWD, ".", O_RDONLY|O_NONBLOCK|O_CLOEXEC|O_DIRECTORY) = 3
fstat(3, {st_mode=S_IFDIR|0755, st_size=4096, ...}) = 0
getdents(3, /* 16 entries */, 32768)    = 432
getdents(3, /* 0 entries */, 32768)     = 0
close(3)                                = 0
fstat(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
write(1, "backups  crash\tlocal  log   metr"..., 49backups  crash     local  log   metrics  run   spool
) = 49
write(1, "cache\t lib\tlock   mail  opt     "..., 43cache           lib      lock   mail  opt      snap  tmp
) = 43
close(1)                                = 0
close(2)                                = 0
exit_group(0)                           = ?
+++ exited with 0 +++
```

Analysis:

The strace appears to be going to the addresses of each directory and checking if the directory exists. It uses the access() call to do so. If the file does exist, it calls openat() to get information on the filename. Mmap reads that information into the process memory of the ls call for later return. The fstat call gives additional information on the files in the directory, which is likely used for output coloration.

At the end, the write call logs any errors and adds to the cache.

3.

strace on inAndOut.o

strace ./inAndOut.o -h

```
execve("./inAndOut.o", ["./inAndOut.o", "-h"], 0x7ffe241ff648 /* 55 vars */) = 0
brk(NULL)                               = 0x557d2113f000
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=86128, ...}) = 0
mmap(NULL, 86128, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f211dc0d000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/usr/lib/x86_64-linux-gnu/libstdc++.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\0\360\303\10\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0644, st_size=1615312, ...}) = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7f211dc0b000
mmap(NULL, 3723296, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7f211d66e000
mprotect(0x7f211d7ec000, 2097152, PROT_NONE) = 0
mmap(0x7f211d9ec000, 49152, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_DENYWRITE, 3, 0x17e000) = 0x7f211d9ec000
mmap(0x7f211d9f8000, 12320, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_ANONYMOUS, -1, 0) = 0x7f211d9f8000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libgcc_s.so.1", O_RDONLY|O_CLOEXEC) = 3
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
fstat(3, {st_mode=S_IFREG|0644, st_size=96616, ...}) = 0
mmap(NULL, 2192432, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7f211d456000
mprotect(0x7f211d46d000, 2093056, PROT_NONE) = 0
mmap(0x7f211d66c000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_DENYWRITE, 3, 0x16000) = 0x7f211d66c000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/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\0\260\34\2\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=2030544, ...}) = 0
mmap(NULL, 4131552, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7f211d065000
mprotect(0x7f211d24c000, 2097152, PROT_NONE) = 0
mmap(0x7f211d44c000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_DENYWRITE, 3, 0x1e7000) = 0x7f211d44c000
mmap(0x7f211d452000, 15072, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_ANONYMOUS, -1, 0) = 0x7f211d452000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libm.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\0\200\272\0\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0644, st_size=1700792, ...}) = 0
mmap(NULL, 3789144, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7f211ccc7000
mprotect(0x7f211ce64000, 2093056, PROT_NONE) = 0
mmap(0x7f211d063000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|
MAP_DENYWRITE, 3, 0x19c000) = 0x7f211d063000
```

```
close(3)                                = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7f211dc09000
arch_prctl(ARCH_SET_FS, 0x7f211dc09d80) = 0
mprotect(0x7f211d44c000, 16384, PROT_READ) = 0
mprotect(0x7f211d063000, 4096, PROT_READ) = 0
mprotect(0x7f211d66c000, 4096, PROT_READ) = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7f211dc07000
mprotect(0x7f211d9ec000, 40960, PROT_READ) = 0
mprotect(0x557d1f8b0000, 4096, PROT_READ) = 0
mprotect(0x7f211dc23000, 4096, PROT_READ) = 0
munmap(0x7f211dc0d000, 86128)           = 0
brk(NULL)                               = 0x557d2113f000
brk(0x557d21160000)                     = 0x557d21160000
openat(AT_FDCWD, "in.txt", O_RDONLY)    = 3
openat(AT_FDCWD, "out.txt", O_WRONLY|O_CREAT|O_TRUNC, 0666) = 4
read(3, "Transmit this message", 8191)  = 21
read(3, "", 8191)                       = 0
write(4, "Transmit this message\n", 22) = 22
close(4)                                = 0
close(3)                                = 0
exit_group(0)                           = ?
+++ exited with 0 +++
```

Analysis

First, there are the standard calls that are executed whenever you make a system call. The strace shows the access of the C++ libraries. At the bottom is the actual program execution with the read/write calls.

ltrace on InAndOut.o

```
ltrace ./inAndOut.o -h
_ZNSt8ios_base4InitC1Ev(0x5651e8ca3019, 0xffff, 0x7ffe9d007970, 128) = 0
__cxa_atexit(0x7f3f388c1f60, 0x5651e8ca3019, 0x5651e8ca3008, 6) = 0
_ZNSt14basic_ifstreamIcSt11char_traitsIcEEC1Ev(0x7ffe9d007650, 0x7ffe9d007958,
0x7ffe9d007970, 160) = 0
_ZNSt14basic_ofstreamIcSt11char_traitsIcEEC1Ev(0x7ffe9d007450, 0x7ffe9d007360,
0x7f3f38baa040, 6) = 0
_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEEC1Ev(0x7ffe9d007430, 0x7ffe9d007360,
0x7f3f38baa040, 6) = 0x7ffe9d007440
_ZNSt14basic_ifstreamIcSt11char_traitsIcEE4openEPKcSt13_Ios_Openmode(0x7ffe9d007650,
0x5651e8aa2115, 8, 6) = 0x7f3f38ba2410
_ZNSt14basic_ofstreamIcSt11char_traitsIcEE4openEPKcSt13_Ios_Openmode(0x7ffe9d007450,
0x5651e8aa211c, 16, 0) = 0x7f3f38ba24d0
_ZSt7getlineIcSt11char_traitsIcESaIcEERSt13basic_istreamIT_T0_ES7_RNSt7__cxx1112basic_string
IS4_S5_T1_EE(0x7ffe9d007650, 0x7ffe9d007430, 0x7ffe9d007430, 0) = 0x7ffe9d007650
_ZNKSt9basic_iosIcSt11char_traitsIcEEcvbEv(0x7ffe9d007750, 2, 256, 0x7fffffffffffffe) =
0x7ffe9d007701
_ZStlsIcSt11char_traitsIcESaIcEERSt13basic_ostreamIT_T0_ES7_RKNSt7__cxx1112basic_stringIS4
_S5_T1_EE(0x7ffe9d007450, 0x7ffe9d007430, 0x7ffe9d007430, 0x7fffffffffffffe) = 0x7ffe9d007450
```

_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_c(0x7ffe9d007450, 10, 0x7f3f38ba24d0, 0x73656d2073696874) = 0x7ffe9d007450
_ZSt7getlineIcSt11char_traitsIcESaIcEERSt13basic_istreamIT_T0_ES7_RNSt7__cxx1112basic_stringIS4_S5_T1_EE(0x7ffe9d007650, 0x7ffe9d007430, 0x7ffe9d007430, 1024) = 0x7ffe9d007650
_ZNKSt9basic_iosIcSt11char_traitsIcEEcvbEv(0x7ffe9d007750, 6, 256, 0x7ffe9d007750) = 0x7ffe9d007700
_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEED1Ev(0x7ffe9d007430, 6, 256, 0x7ffe9d007750) = 0
_ZNSt14basic_ofstreamIcSt11char_traitsIcEED1Ev(0x7ffe9d007450, 0x5651e9838018, 0x5651e9838010, 1) = 19
_ZNSt14basic_ifstreamIcSt11char_traitsIcEED1Ev(0x7ffe9d007650, 0, 18, 0) = 17
+++ exited (status 0) +++

Analysis

The ltrace output is very informative. It shows the calls to the compiled binary libraries such as ifstream. Using a disassembler on these libraries would allow someone to determine what is happening via analyzing the assembly code. From what can be seen just from ltrace output, we can be certain there is an input and output stream.