B4 - Unix System Programming

B-PSU-402

strace

System call retrieval

2.3

strace

binary name: strace
language: C
compilation: via Makefile, including re, clean and fclean rules

- The totality of your source files, except all useless files (binary, temp files, obj files,...), must be included in your delivery.
- All the bonus files (including a potential specific Makefile) should be in a directory named *bonus*.
- Error messages have to be written on the error output, and the program should then exit with the 84 error code (0 if there is no error).

You must complete this project on at least x86-64/Linux.

The following libraries are allowed: **libc**, **libelf**, **libm**.
The use of **PTRACE_SYSCALL** and **PTRACE_SYSEMU** are forbidden.

strace traces a prgram in real time and displays all of the system calls it executes in their order of appearance.

Develop an alternative to strace that implementing the following options:

- **-p**: force a specific PID instead of executing a command
- **-s**: display the detailled arguments (see below).
  By default, your strace must only display the arguments and return values in hexadecimal form.
  If the system call has a void return value, display a question mark.
  With **-s** option, your program must be as close as possible to the *strace* command on your system, and therefore display the following:
    - integers in decimal form,
    - pointers on a character string in the form of a character string,
    - detailed structures (value for each field).

```
Terminal
~/B-PSU-402> ./strace --help
USAGE: ./strace [-s] [-p <pid>|<command>]
```

Here is an output example for a single system call, without the **-s** option:

```
Terminal
write(0x1, 0x7ef23a43, 0x4) = 0x4
```

Here is a list of possible **bonus** points:

- Handle the flags
- 32-bit (x86) comptability
- Compatible on different material structures (ARM, PowerPC, SPARC etc.)
- Compatible with different systems