CS220 - Computer System II
Assignment 12 (100 points)

Due: 11/23/2016, 11:59pm

1 Question 1 (100 points)

In this assignment, you will mimic the job of a binary loader (in a highly simplified manner). You will write a program that will load code from a file, and execute the code. You will be provided a function signature and a binary file that contains the raw bytes of the function's code. The function is a pre-compiled 32 bit binary. It is not an elf binary. It contains the raw bytes of a calculator function. It has been tested on remote.cs.binghamton.edu.

File `func.bin` contains a function with signature `int calc(char operator, int num1, int num2);`. Implement the main function within loader.c. NOTE: The below instructions are only pointers to help you get started. You are encouraged to experiment and try different library functions. For example, you may want to experiment with open and read instead of fopen and fread. Or, if you feel adventurous, you may want to allocate memory on the heap, read the raw bytes on to the heap, call `mprotect` to make the page that contains the raw bytes executable, and execute it.

- The main function must accept exactly 4 arguments. Otherwise, main must print "Usage" message and exit. The first argument is the name of the file that contain the binary function, the second argument and fourth argument are integers, and the third argument is a character that represents an operation.
- Main function will open the file with first argument as the name. HINT: use fopen. The second argument to fopen is the mode in which the file is opened. Because you are opening a binary file, the mode must be "rb". Refer man page for fopen for more details.
- Main function will read the contents of the file into a local array that is large enough to contain the entire file. HINT: use fread. You could either read character by character or first calculate number of bytes in the file, and read them all in one call to fread. Refer to man page for fread for usage.
- Declare a function pointer type with name "Calc_fptr" with the same signature as calc.
- Convert the 2nd and the 4th arguments to integers using function "atoi". Refer to the man page of atoi for usage.
- Cast the array to type "Calc_fptr". Invoke it with the 2nd, 3rd and 4th arguments to main as arguments.

- Write a Makefile to compile loader.c to generate the program "loader". You will get a segmentation fault when you run loader with the right arguments. This is because, you are trying to execute code that is in the local variable, which is on the stack. Stack is not executable. Now, modify the Makefile and include `-Wl,-z,execstack` flag. This is a linker flag that tells the linker to mark the stack region as executable. This is for demonstration only. DO NOT use it in production code, if you were ever to write code for a profession.
- Print the result, and return.

2 Skeleton Code

```
/* TODO: Include appropriate headers */

int main(int argc, char *argv[])
{
  /* TODO: Declare an array large enough to hold the raw bytes. Raw bytes are
     best stored in byte-addressable arrays. Pick the appropriate type. Call
    it "raw_bytes"*/
  /* TODO: Declare a function pointer type that matches the calc function's
    type. Call it  "Calc_fptr" */

  FILE *fp;
  unsigned int i;
  Calc_fptr calculator;

  /* TODO if number of arguments is not 4 (5 including program name)
     print ("Usage %s <filename> <uint> <operation> <uint>\n", argv[0]) and
    exit */

  /* TODO: Open and read the binary file into raw_bytes. Use fopen and fread.
     */

  calculator = (Calc_fptr) calcfunc;
  /* TODO: Print the result. Refer to sample input and output. */
  return 0;
}
```

3 Sample input and output

```
$ ./loader
Usage ./loader <filename> <int> <operation> <int>
$ ./loader func.bin 32 + 11
32 + 11 = 43
$ ./loader func.bin 32 - 11
32 - 11 = 21
$ ./loader func.bin 32 * 11
Usage ./loader <filename> <int> <operation> <int>
$ ./loader func.bin 32 \* 11
32 * 11 = 352
$ ./loader func.bin 32 / 11
32 / 11 = 2
$ ./loader func.bin 32 / 0
Floating exception
```

Input "32 * 11" is a strange one. The terminal replaces * with all the files in the directory, so you must escape it!

4 Submitting the result

Create a directory Assn12 and store loader.c and Makefile in Assn12.

```
$ tar -cvzf assn12_submission.tar.gz ./Assn12

```

Submit assn12.tar.gz on Blackboard.