CS220 - Computer System II
Lab 4

Due: 09/28/2016, 11:59pm

1 Introduction

In this lab, you will play with pointers, structures and unions.

2 Getting Started

Download lab4.tar.gz and extract it. Inside, you should find main.c, secret.c, secret_obj.o and secret.h.

3 Pointers

1. Write the following program ptrs.c, insert a print statement to print the address and values of a, b, c and d. Use format specifier %p to print addresses and %x to print values.

```
int main() {
  int    a =  0xe;
  int   *b = &a;
  int  **c = &b;
  int ***d = &c;
}

```

2. In C, 'const' is a keyword used to indicate immutability. You are to investigate the difference between 'const int *p1' and 'int const *p2'. Write a program const.c that declares p1 and p2, alters the values of p1 and p2, and values that p1 and p2 point to (e.g., p1++, (*p1)++). Record your response in lab4.txt. Indicate whether or not p1, p2, *p1 and *p2 can be altered.

3. You will write a program print_main.c to print the bytes corresponding to main function's code. Compile it using `gcc -std=c89 -o print_main print_main.c` Note that the code is in .text section and is readable. So, in principle, we should be able to read and print the contents of main.

```
int main()
{
```

```
  /* declare unsigned character pointer ptr */ = &main;
4 do {
    /* print value pointed to by ptr as a hex value */
6   } while ( *ptr != /* Return byte */);
  }
8
```

HINT: Cast address of main to be a pointer to unsigned char array. Print all characters as hex values till you find a return statement. Return in x86 is incorporated using a one byte instruction 0xc3. Therefore, once you find 0xc3, print it and stop. You can verify your output by comparing it against the bytes of main obtained through `objdump -d print_main`. What happens if you change the contents of main through (e.g., *ptr = 0;)? Record your findings in lab4.txt.

4. You are provided with secret_obj.o, secret.h, secret.c and main.c. File secret.h contains the structures and declarations of functions defined in secret_obj.o. You are also provided with secret.c that shows the program logic of get_keeper function in secret_obj.o. Your task is to implement extract_secret function in main.c to find the value of secret. You can compile main using `gcc -o secret main.c secret_obj.o -std=c89`. NOTE: The secret is not the same for all students, so don't be surprised if your friend gets a different answer! You are also provided with function verify_secret in secret_obj.o. Use it to verify your solution.

4 Submitting the result

Create lab4_submission.tar.gz file comprising Lab4.txt, ptrs.c, const.c, print_main.c, secret.h, main.c and a makefile to compile main.c. Upload the files to Blackboard.