

CSCI3240 Project 2: Reverse Engineering

1 Introduction

This project gives you a chance to reverse engineer a set of four mystery functions from disassembled machine code (Project2.s). Your task is to first identify what each mystery function does and then write an equivalent C code. You don't need to directly translate the assembly code to C.

2 Logistics

This is an individual project. All handins are electronic. Clarifications and corrections will be posted on the course D2L page.

3 Handout Instructions

Download the Project2.zip:

Goto D2L → Course Page → Content tab → Table of Contents → Projects → Project 2 → Project2.zip

Start by copying Project2.zip to a (Protected) directory on a Linux machine in which you plan to do your work. Then give the following command:

```
\$ unzip Project2.zip
```

This will cause two files to be unpacked in the directory: Project2.c and Project2.s. The only file you will be modifying is Project2.c.

The Project2.c file contains a skeleton for each of five mystery functions. The assembly code for each of the mystery functions are provided in the Project2.s file. Your assignment is to analyze the assembly code and identify what each mystery function intend to do. You will next, write the equivalent c code for each mystery function. Again, you don't need to directly translate the assembly code to C.

4 Evaluation

Your score will be computed out of a maximum of 100 points based on the following distribution:

- 20 Correctly identifying the mystery functions.
- 20 Detailed documentation on your approach.
- 50 Correctness of the C codes.
- 10 Insightful comments and programming style.

5 Handin Instructions

1. You need to submit two files.
 - a. `Project2.c`: You will write the c codes for the mystery function here.
 - b. `Project2Description.pdf`: In this document, you will provide:
 1. The description of what each mystery function does.
Example:
MysteryFunction1: Explain what MysteryFunction1 does here.
MysteryFunction2:
MysteryFunction3:
MysteryFunction4:
MysteryFunction5:
 2. Discussion on the approach(es) that you used to identify what the mystery function does.
2. Do not zip the submission.
3. Provide adequate comments on your c code.
4. Upload the requested files in “**Project2**” dropbox in D2L.