Homework 6: Code Injection
CPE221

Instructor: Rahul Bhadani

Due: April 13, 2025, 11:59 PM
80 points

You are allowed to use a generative model-based AI tool for your assignment. However, you must submit an accompanying reflection report detailing how you used the AI tool, the specific query you made, and how it improved your understanding of the subject. You are also required to submit screenshots of your conversation with any large language model (LLM) or equivalent conversational AI, clearly showing the prompts and your login avatar. Some conversational AIs provide a way to share a conversation link, and such a link is desirable for authenticity. Failure to do so may result in actions taken in compliance with the plagiarism policy.

Additionally, you must include your thoughts on how you would approach the assignment if such a tool were not available. Failure to provide a reflection report for every assignment where an AI tool is used may result in a penalty, and subsequent actions will be taken in line with the plagiarism policy.

Submission instruction:

Upload a .pdf on Canvas with the format {firstname.lastname}_CPE221_hw06.pdf. For example, if your name is Sam Wells, your file name should be sam.wells_CPE221_hw06.pdf. If there is a programming assignment, then you should include your source code along with your PDF files in a zip file {firstname.lastname}_CPE221_hw06.zip. Your submission must contain your name, and UAH Charger ID or UAH email address. Please number your pages as well.

1 Injecting ARM Code into Memory

Consider a C code:

1.1 C Code:

```
#include <iostream>
using namespace std;
int main()
{
     //m is a globally-accessed variable
     //You can assume it is in some register R0
    int m = 35;
    // even
    if(m%2 == 0)
    {
        m++ ;
    }
    else
    {
        m--;
    }
}
```

Your job is to inject the above code starting from the memory address 0x40404040. The idea here is that when the program counter (PC) is set to 0x40404040, the injected code will be executed.

To approach this problem:

1. You will first be required to write an ARMv7 code. For this purpose, you don't need to consider including the `done:   B done` statement in your ARMv7 code. **(20 Points)**
2. Then you need to determine the hex code for each instruction. **(20 Points)**
3. Finally, you need to copy the hex code corresponding to those instructions into the required memory locations. **(20 Points)**
4. To test if your code injection is successful or not, explicitly set the PC register value to 0x40404040. **(20 Points)**