CPE 325: Embedded Systems Laboratory
Laboratory Assignment #11

1. Assignment [100 pts]

1. There are 2 questions embedded inside the tutorial for Lab 11. Answer them in your report. **[2 X 10pts = 20Pts]**
2. Find the executable ***crack_me/Lab11_crack_me_<your id>.out*** under the Canvas files tab. This executable file has several usernames and passwords.
    a. Find as many correct passwords that you can find. Document the entire process in your report and elaborate to your instructor during demonstration.
    b. Connect the 4618 board to the computer. Make the UART connection at a baud rate of 115,200.
    c. Program the board with the provided .out file and try to guess the correct password. Upon successfully guessing the password, you will see "`Correct!`" message. Take a screenshot and put it in your report. **[20 pts]**
3. From the same .out file from Q2, find the following relevant information. What tool did you use? Take a screenshot and put it in your report.
    a. What is the magic number used? **[1 pts]**
    b. What is the class of this *.out* file? **[1 pts]**
    c. What machine was this file built for? **[1 pts]**
    d. What is the size of the header? **[1 pts]**
    e. How many section headers are there? Please verify. You may need to run the command again. **[6 pts]**

4. You are given an executable file **Lab11_*reverse_me.txt***. This is a hex file generated using the process described in Section 5.1 in the tutorial.
    a. Program the given hex file to your microcontroller using the MSP430Flasher tool and paste the output in your report. **[10 pts]**
    b. Guess from observation on the board what the program does? **[5 pts]**
    c. Using the naken utility and the steps shown in Section 5.2 of the tutorial, reverse engineer the hex file to assembly code. **[5 pts]**
    d. Comment on each line of the assembly code generated from Q4c above to describe what each line is doing. **[20 pts]**
    e. Describe what the program is doing in a neat flowchart. You can also write a paragraph to describe in addition to the flowchart. **[10 pts]**

2. Bonus

Change any functionality of the code provided in the hex file. Program the new hex file and show it to your instructor. Or alternately discuss it in your report with a demonstration video. You are free to change anything in the hex file provided it produces a functioning hex file, and you know exactly what functionality you changed. **[10 pts]**

3. Deliverables

1. Report with multiple screenshots for each of the problems mentioned above.

4. Theory

1. ELF File components
2. Naken Utility
3. MSP430 Flasher