

# CPE 325: Embedded Systems Laboratory

## Laboratory Assignment #10

### Assignment

**[100 pts]**

1. There are at least 5 questions embedded inside the tutorial for Lab 10. Answer at least 4 of them. **[4 X 5pts = 20Pts]**
2. Please find the executable file *crack\_me.out*. This executable file has bunch of usernames and passwords.
  - a. Find as many username and password that you can find. Document the entire process in your report and elaborate to your instructor during demonstration.
  - b. Connect your MSP-EXP430F5529 board to your computer. Make the UART connection at 115200 baudrate.
  - c. Program the board with the provided .out file and try to guess the correct password. Upon successful guessing the password, you will see "and its CORRECT!!!!!!!!!!!!!!" message. Take a screenshot and put it in your report.
  - d. *Instructor may give you a new executable during demonstration. You must be able to crack the new executable upon asked.* **[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 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 many need to run the command again. **[6 pts]**  
*Instructor may give you a new executable during demonstration. You must be able to crack the new executable upon asked.*
4. You are given an executable file *reverse\_me.txt*. This is a hex file generated using the process described in Section 5.1 in tutorial.
  - a. Program the given hex file to your microcontroller using MSP430Flasher tool, and paste the output in your report. In your demonstration, you must show the whole process. **[10 pts]**
  - b. Guess from observation on the board what the program does? **[5 pts]**
  - c. Using the naked 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]**

## 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 as long as it produces a functioning hex file and you know exactly what functionality you changed. **[10 pts]**

## Deliverables

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