CPE 325: Embedded Systems Laboratory
Laboratory Assignment #11

Assignment [100 pts]

1. **[50 pts]** Find `crackMe/<your-name>.out` file in the Files section of Canvas. Find the processor architecture that this executable file was made for. You should use one of the GNU binary utilities for that.

   The program is designed to prompt you to enter a password (you need UART connection with the PC at the baud-rate of 115200). Guess the correct password. Use one of the GNU utilities to print all the strings defined in the data section of this executable file. Your password might be one of them.

   Load the executable to the micro-controller using Code Composer Studio and try your passwords until you can crack it. You will see "You cracked CRACKME!!!" as output on successful guess.

2. **[50 pts]** Find `reverseEngineerMe.txt` file in the Files section of Canvas. This file is in hex format and it was obtained by reading the flash memory of MSP430 microcontroller, using MSP430Flasher Utility. You need to use the `naken_utility` to dissemble this code (i.e. generate assembly code from the hex file), and reverse engineer what the program does. The hex file contains initialization code that starts with initializing the stack pointer register. You can ignore this part of the program when doing reverse engineering.

   Load the hex file to the Experimenter board using MSP430Flasher Utility, and observe the functionality of the program. Do your observations support the results of reverse engineering? Demonstrate the loaded program to your instructor (this is the only thing you need to demonstrate for this this lab).

Deliverables

1. Lab report which includes:
   a. Target architecture name for the binary file from part 1.
   b. Screenshots of failed and successful attempts from part 1 (make sure they include the correct password).
   c. Disassembled code from part 2.
   d. Detailed description of what the program from part 2 does.