CS 490 / ECE 492: Embedded Systems Security

Low-Level Interfacing and Secure Passwords #06

Total Points: 100

Assigned Date : Monday, March 14, 2016
Due Date : Monday, March 20, 2016 @ 11:59:59 a.m. [**Group assignment**]

1 Low Level Interfacing

You should now have a working, authenticated web interface for your temperature sensor/stepper motor console. We are now going to experiment with a common modality in embedded systems design. That is low level interfacing with other devices. Specifically, in this lab we are going to interface our BeagleBone with an external EEPROM. Why? Many microcontrollers don't have their own non-volatiale storage, and so this is done through external chips. For the first part of the assignment, you should wire up the I2C EEPROM according to the diagram shown below. Write a program that can read and write arbitrary data to the I2C EEPROM. Be sure you know how to use the i2cdetect program to show the I2C address of your device.

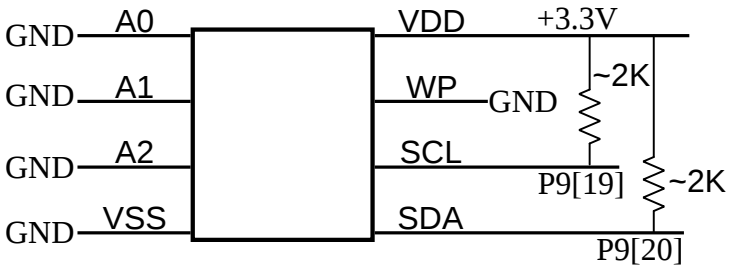

Figure 1: Wiring for EEPROM

2 Password Hashing

At this point, you should be able to read and write to your I2C EEPROM. Good. Now, use the I2C EEPROM to store the password file that is used to access the web interface for your motor/temp sensor combo. Your password file should have the following format: *username:salt:pwHash* for each user that is allowed access to the server. Use at least a 32-bit cryptographicallly secure randomly generated salt. Also, use a known, secure hashing algorithm with sufficient complexity (ie. bcrypt, scrypt, or PBKDF2).

3 Encryption of EEPROM

At this point, you are getting better, but it would be nice if your file was actually encrypted. Use symmetric key encryption to encrypt the contents of your EEPROM. Think carefully about how you will do key storage. You should be able to prove that your EEPROM is encrypted, and you should still be able to use it to authenticate users to the web server.

Deliverables

The due date of this assignment is **Monday, March 20, 2016 @ 11:59:59 a.m.** A dropbox will be opened for submission on Moodle before the due date. You are required to detail your findings in a report. All reports must be in **PDF** format. No exceptions.

- [**50 points**] A group demo of your work. We will again ask you questions on what you've done and how you've done it.
- [**45 points**] A group report with the followings:
  - Motivation and objective of the experiment.
  - A detailed methodology of your experiment. You must be able explain the commands, tools, procedures you've used. Don't simply list the commands. We want you to explain what you've done and why you did it. Screenshots highly recommended.
  - A detailed testing plan and test results.
  - Justification of your observations. You must be able to justify and/or argue why (or why not) your method worked.
  - Final conclusions.
- [**5 points**] An individual report. Use this report to explain your individual contributions towards the experiment. This is a separate writing on your own. In essence, both members of the group will write their own individual report and make their own submission; you are only required to submit one group report. You can use the individual report to explain/mention/complain about your teammate's contributions to the project as well.