CS 490 / ECE 492: Embedded Systems Security
SPI and Non-Standard Wireless #07
Total Points: 100

Assigned Date : Monday, March 28, 2016
Due Date : Wednesday, April 06, 2016 @ 11:59:59 a.m. [**Group assignment**]

1 SPI Interfacing

The SPI protocol is another low-level, hardware protocol for communication between ICs. It is different from I^2C in that the speed and data format are entirely device dependent, so it allows for much faster data transfer from device to device. That said, it does require a few more wires than I^2C, and most of these are uni-directional:

- **MOSI** is *Master Out Slave In* which is used to transfer data from the master to the slave device;
- **MISO** is *Master In Slave Out* which is used to receive data on the master which is sent by the slave;
- **SCLK** is *Serial Clock* which is generated by the master to synchronize bit transfers; and
- $\overline{\textbf{CS}}$ is *Chip Select* which is used by the master to select an external device for communication (especially if more than one are connected).

SPI is used in many modern devices due to the ease of integration with ICs, and that there is no inherent max. speed defined by the protocol. In fact, some SD cards use SPI. In this lab, we will be using a wireless radio, the nrf24L01+, which is a SPI device. The nrf24 radio operates in the 2.4 GHz spectrum over 126 selectable channels, and has a range of about 50 feet encumbered, and about 200 feet in open air. The datasheet for the radio can be found here https://www.sparkfun.com/datasheets/Components/SMD/nRF24L01Pluss_Preliminary_Product_Specification_v1_0.pdf.

In this part of the lab, we would like you to get communication of your nrf24L01+ working with another group in the lab. The nrf24L01+ radios require matching parameters (ie. channel, address, payload length), so agree upon these parameters with your neighbor first. **Do not use defaults found with example code! This is bad security practice.** You should read and understand the datasheet well enough to set up your own configuration. Configure the radios to send and receive commands to read your temperature sensor and/or spin your motor, just like you would have done through the web interface.

2 Security of the nrf24L01+

For this section, we want you to analyze the security of the nrf24L01+ radios. As you will no doubt tell from implementing Part 1, there are quite a few parameters to using these radios. You should attempt to see if there is any authentication between radios, if any encryption is used at the hardware level, if the data can be intercepted, replayed, etc. Can the radios be reprogrammed over-the-air?

Attempt to read, spoof, impersonate, etc. another group in lab **WITHOUT** discussing with them. Ostensibly, there should be subtle variations within each pair's set of commands, as well as addresses, channels, etc. You can also attempt to look around at home to see if you have a commercial device that uses these radios and attempt to reverse engineer this device.

Deliverables

The due date of this assignment is **Wednesday, April 06, 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.