Title of the Experiment: Bus Snooping Attacks

Group Members' Names: Sujan Kumar Saha, Pankaj Bhowmik

Date: 09/17/2019

Abstract

This experiment is about bus snooping attack. The off chip buses are open on the PCB board. So by physical access to a PCB board, it is possible to see the information passing from one component to another. If any secret information is passed from one component to another and not encryption is done, then by bus snooping attack it is possible to get the information without using any software. In this experiment, we have used the Hardware Hacking board (HaHa) and did the bus snooping on the data and clock bus lines from microcontroller to accelerometer. We changed the position of the board which changes the data value sent for the accelerometer. We were able to observe the changes of those data values and get the value by snooping the bus.

Experiment Details

Goals: The goal of this experiment is to investigate how to snoop off chip buses and decode the data on bus lines

Experimental Setup: We used Hardware Hacking (HaHa) board, analog discovery and waveform on a computer for this experiment

Experiment Steps:

1. We have loaded the given code to ATmega16 microcontroller.
2. We connected the channel 1 and channel 2 of the oscilloscope to SCLK and MISO pin of the SPI to observe the data being passed from the accelerometer to ATmega16.

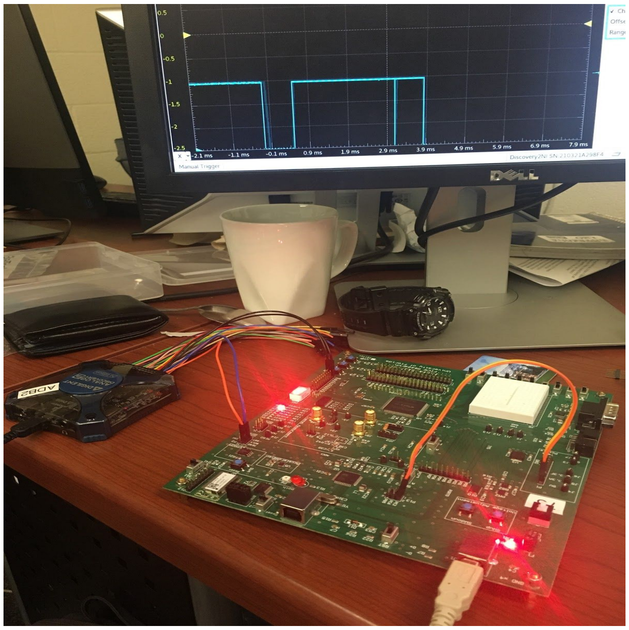

Figure 1: Experimental setup

Results and Observations

After observing the bus signals on waveform, we have the following insights discussed below.

1. The SCLK is the clock line. The clock frequency of the SCLK is 7.69 KHz.
2. The MISO pin is the data line. We observe data bits on MISO pin which is used to send data from accelerometer to Atmega16. Here, Atmega16 is master and accelerometer is slave.
3. Yes, it's possible to set up the oscilloscope to trigger the data bus line and decode the data. We have attached the screenshot below in figure 2. Here, the SCLK clock is triggered at the rising edge of the overall clock of the board which is 1Hz.

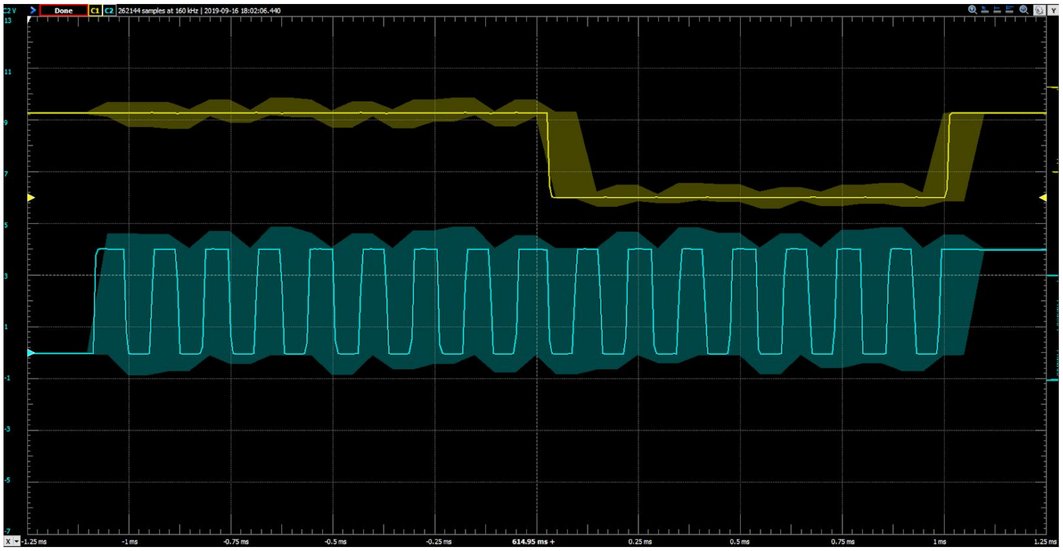

Figure 2: The SCK and MISO signal on channel 1 and channel 2 of the oscilloscope

4. Yes, the general data packet format is 8 bit. We observe 16 clock cycles in the SCLK. Last 8 clock cycles are used to send data using MISO pin and first 8 cycles are used to send data from ATmega16 to accelerometer using MOSI pin. We have attached two screenshots in figure 2 and figure 3 to show that. We tilted the tilted the position of the board and observe the change of the data on the MISO pin. Initially, it was “00000000”. But the other data are “11000101”, “00000010” and “01000000” in figure 4, 5 and 6 respectively.

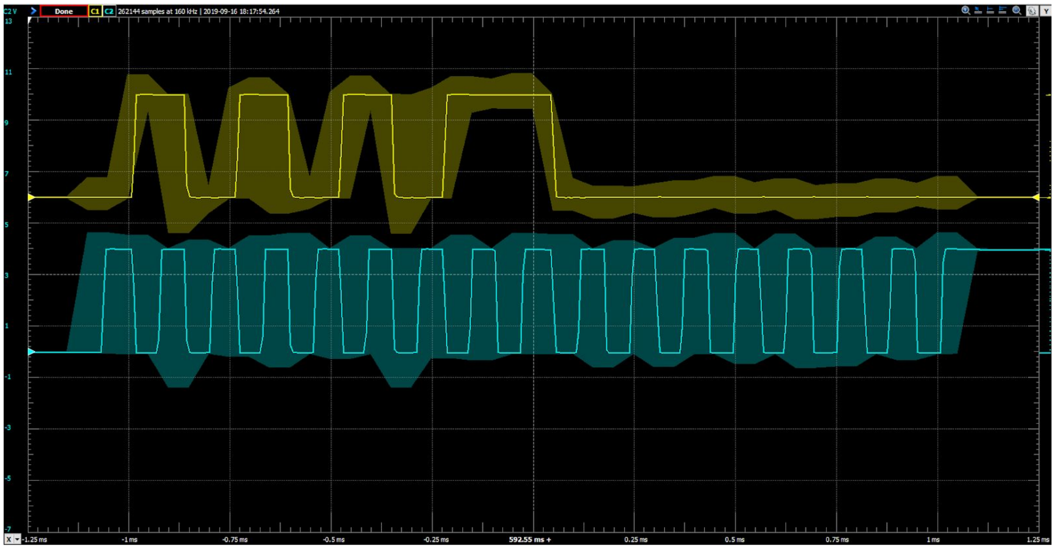

Figure 3: The SCLK and MOSI signal on channel 1 and channel 2 of the oscilloscope

5. If I don’t have convenient labeled traces to probe the clock and data lines on the board, the easiest way is to look at the important chips first (e.g. MAX 10 FPGA, ATmega16 and EEPROM, etc on HAHA board), then figure out the input output pins and probe on those pins. The other way is to check if the bus lines on the PCB can be probed or not. If the bus lines don’t have insulators, then it is possible to probe directly from the bus lines.
6. To prevent such attacks, one approach can be to use insulator for each input output pin of a chip just after coming from the chip so that the attacker can not probe on the pins. Also, another approach will be to layout the off chip buses on the PCB in such a way that the bus lines are not visible to the users. By using these approaches, it is possible to prevent off chip bus snooping attack. But it will be hard to debug any signal after packaging the chip and bus lines on PCB. In this case, it is better to print the PCB in two steps. In the first step, the PCB is designed without using any insulator on the pins and bus lines. In the second step, after doing all testing on the buses and chips, the insulation can be done.

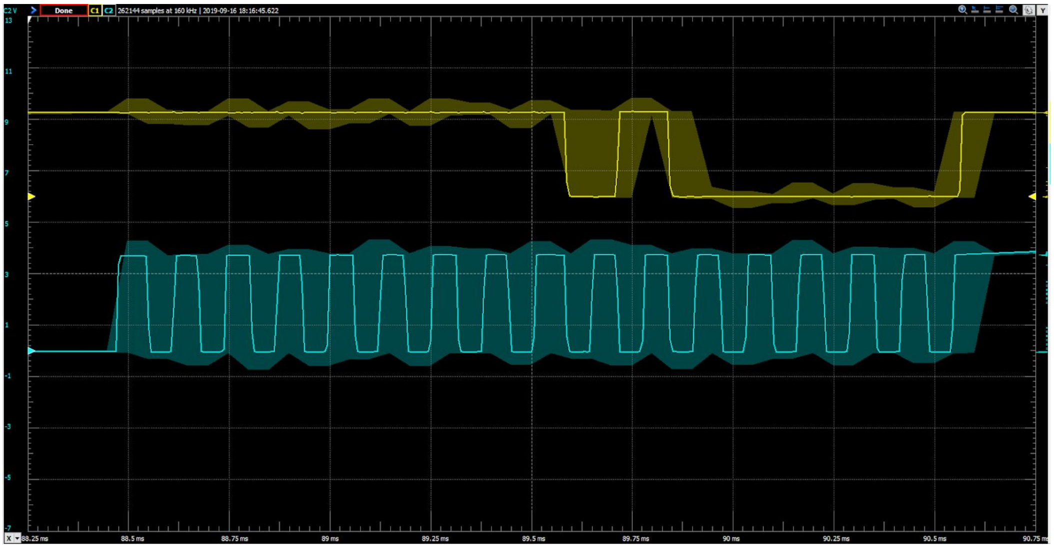
262144 samples at 160 kHz | 2019-09-16 18:16:45.622

Figure 4: The change of data pattern on MISO after tilting the board

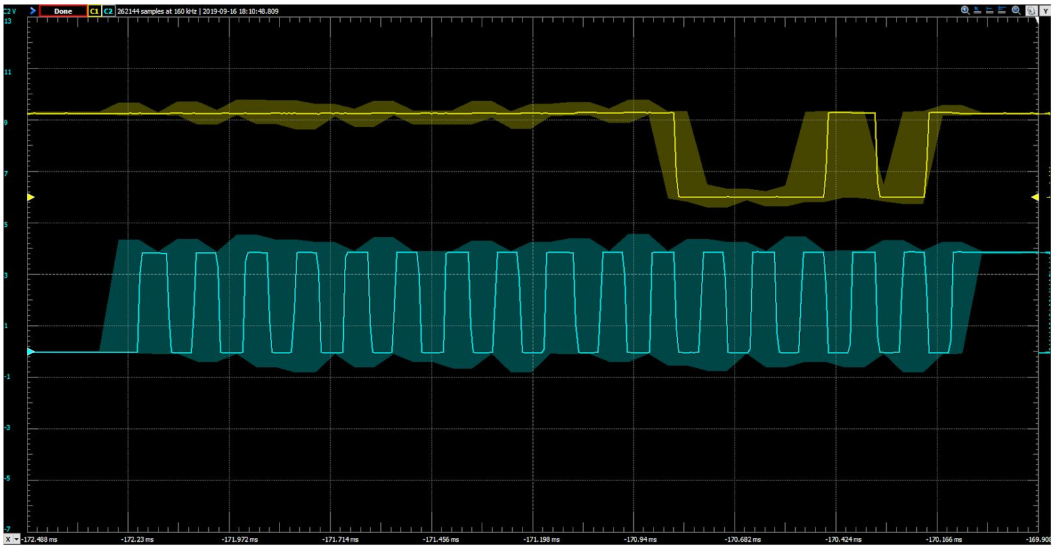
262144 samples at 160 kHz | 2019-09-16 18:10:48.809

Figure 5: The change of data pattern on MISO after changing the position of the board

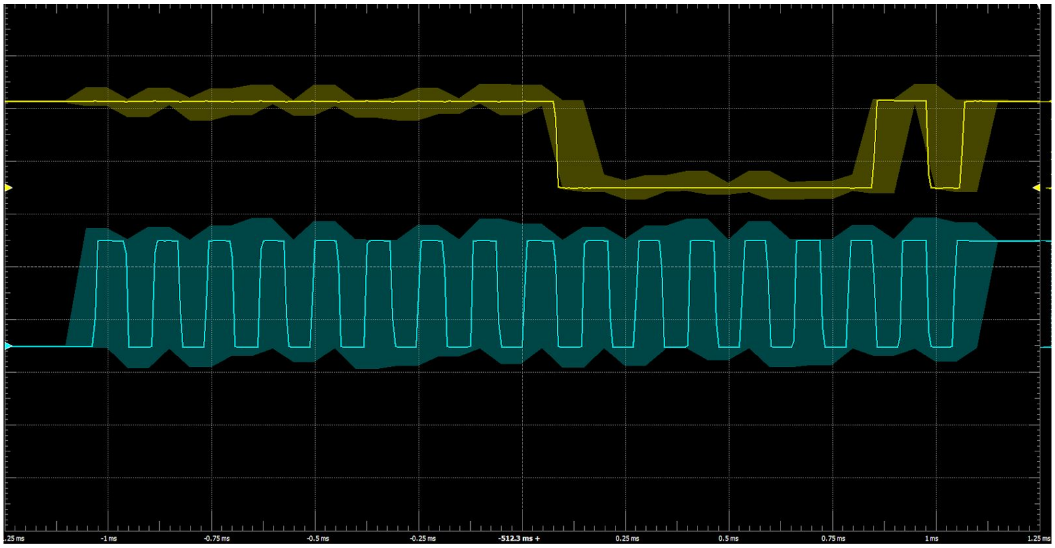

Figure 6: The change of data pattern on MISO after changing the position of the board

Discussion and Summary:

Interesting observation: Initially when we were trying to observe the signals, we got the SCLK bus signal as a clock with 1Hz. But this should not be a SCLK clock frequency. After that we zoomed the signal and saw that when the 1Hz clock triggers at its rising edge, the SCLK clock starts. We can see the 16 clock cycles of the SCLK which has higher clock rate.

Summary: By running this experiment, we learned about bus snooping attack and how to decode important information by physical access to the board. We suggested some solution for that. There may be some other solution too. Overall, it was a good experience for us to launch a physical attack on board that we did not do before.