EECE 5698 Fall 2025
Lab 1: Introduction to Electronic Benchtop Tools for Measuring Embedded Security

Instructor: Prof. Kevin Fu
TAs: Hui Zhuang, Nuntipat Narkthong
Last updated: 09/12/2025, 8 PM

7 points total
Submission Deadline: Sept. 22, 11:45 AM.
Submit your report as an individual on Canvas.

Equipment

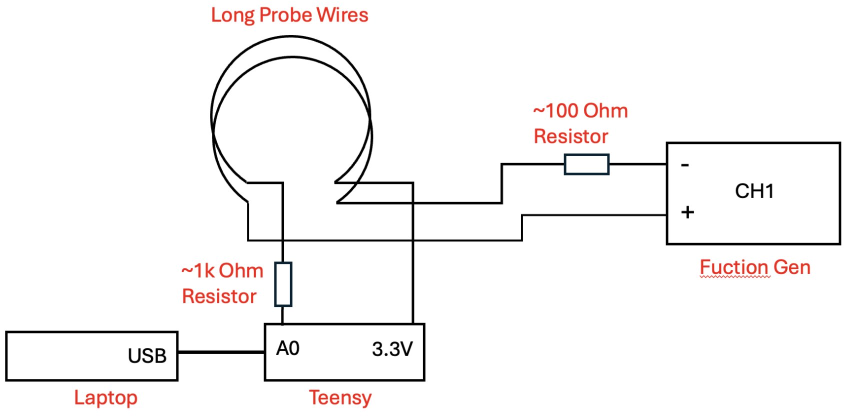


Fig. 0. Connection Diagram

- Two long probes made of jump wires (#1 in Fig. 1; you need to make it by yourself)
- Teensy 4.0 board (#2 in Fig. 1, specs and pinouts can be found here)
- ~100 Ohm and ~1k Ohm resistor (#3 in Fig. 1)
- Function Generator Agilent 33220A (Use Sine output, 15 MHz, and 10 Vpp for this lab)
- Your laptop

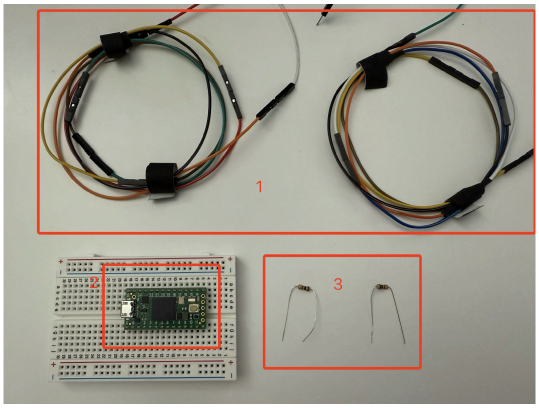


Fig. 1. Main Components

Notes

- When you take screenshots on your laptop, reduce the size of the app window (see Fig. 2 for example) so that the texts are relatively larger and more readable for grading.

Problem 1. Build your sensor

In this lab you will use Teensy's internal ADC to measure the characteristics of the Teensy 4.0 board's 3.3V (100mA max) output. **Essentially, you can regard the system consisting of your laptop, Teensy's ADC, and long probe wires as a simple sensor you have created using off-of-the-shelf devices.** This lab is gonna show you how sensors with design flaws can be unreliable under simple sensor injection attacks.

Step 1: Build the long probes

> The two long probes are basically loop antennas. You will not see such an apparently flawed design in an industrial product, of course. But this helps you quickly understand what a sensor injection attack is by "magnifying" the flaws.
>
> Use 7 or 8 jump wires to build each long probe. Connect the jump wires and then use gaffer tapes to fix them if needed. Make sure each long probe has at least 3 windings, as shown in Fig. 1. Then connect one long probe with the Teensy's Internal ADC (Pin A0), and the other one with the function generator as shown in Fig. 0.
>
> Finally, place the two probes together so they act like tightly coupled inductance/loop antennas, as shown in Fig. 3.

Step 2: Setup up the remaining things

Now you need to finish the remaining connections as shown in Fig. 0. Basically, your Teensy's ADC uses one long probe to measure the output voltage of Teensy 4.0. But meanwhile the long probe is subjected to intentional electromagnetic interference/injection (IEMI) generated by a nearby function generator.

Remember to power up Teensy 4.0 by connecting its USB so that Teensy can output a 3V DC. Then use the Python on your laptop to see Teensy ADC's measurements.

Let's first use your Teensy's ADC to measure what the output voltage is like when there is no intentional interference. **Disable your function generator output.** Please upload and run Lab01.ino using Arduino IDE, and run this Python Script to observe the signal in real time. **Remember to replace the port number in the Python script with the port of your device**. When you want to stop running the program, simply close the plot window to exit. As shown in Fig. 2, you should be able to observe that the signal is distributed around 3.3V, which corresponds to the output voltage of the Teensy 4.0 board. After the program ends, you can also **observe the overall sample information in Terminal, including the maximum value, minimum value, and average value**, as shown in Fig. 3**.**

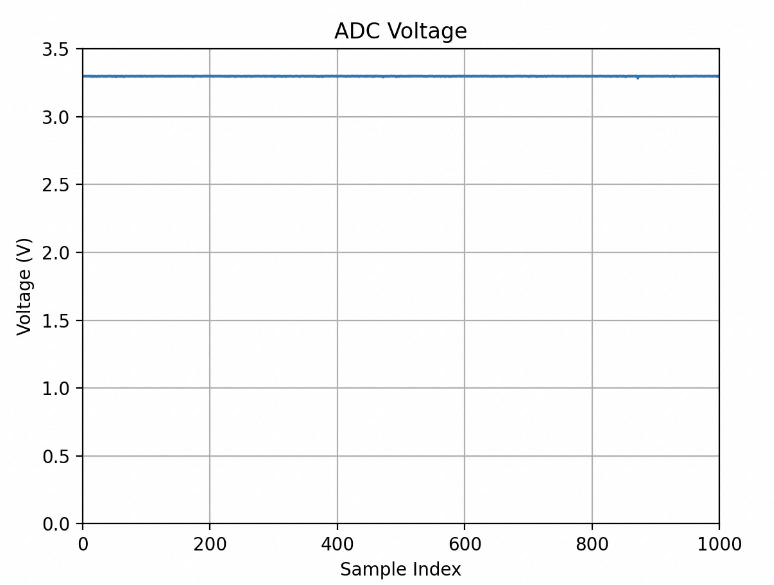
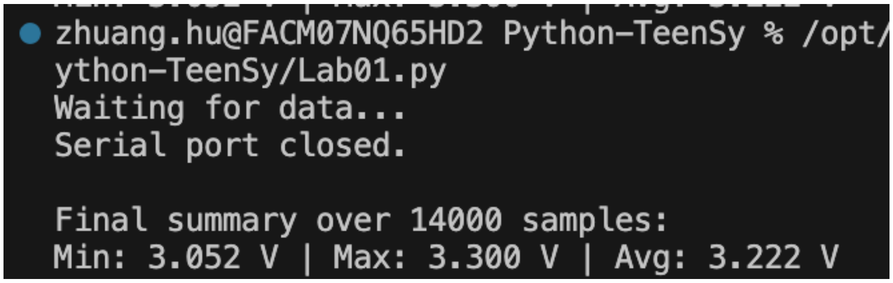


Fig. 2. IEMI OFF



```
● zhuang.hu@FACM07NQ65HD2 Python-TeenSy % /opt/
  ython-TeenSy/Lab01.py
  Waiting for data...
  Serial port closed.

  Final summary over 14000 samples:
  Min: 3.052 V | Max: 3.300 V | Avg: 3.222 V
```

Fig. 3. Overall Samples Information

Question 1 (2 pts):

- Submit a screenshot similar to Fig. 2 when the IEMI is off.
- What are the min, max, and average in your case?

Problem 2. Sensor injection attack with IEMI

Let’s see what happens when an adversary performs an IEMI attack against your sensor.

As mentioned before, arrange the two long probes in the same way as Fig. 4 so that the EM coupling between the attack’s signals (the function generator’s output) and the victim sensor’s signal input are maximized.

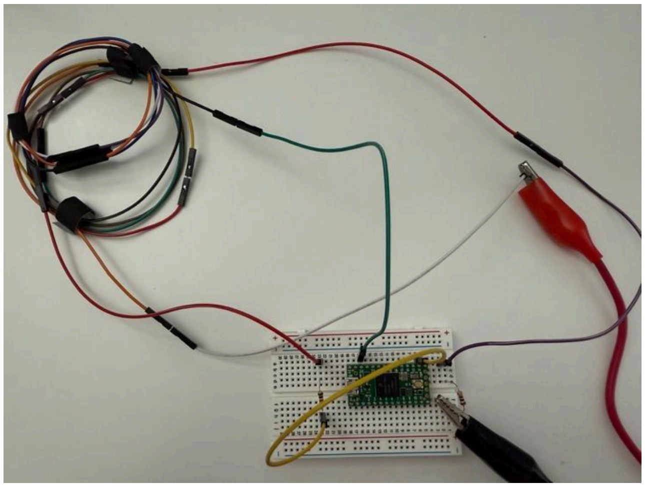


Fig. 4. Setup for demonstrating the strongest attack

Then, simply turn on your function generator output and run previous Python Script. You should observe an increased range of variation of the voltages, as shown in Fig. 5.

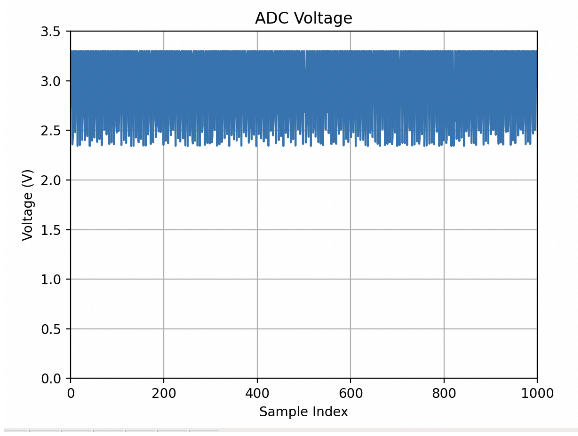


Fig. 5. IEMI ON, tight coupling.

Question 2 (2 pts):

- Submit a screenshot similar to Fig. 5 when the IEMI is on with the strongest coupling between the two long probes.
- What are the min, max, and average in this case?

Besides 15 MHz, you can tune the injection signal frequency and see how the variation changes. Try to map what you observed to the concept of frequency response introduced in Lab01Prelab and understand the role of frequency in analog sensor security.

Problem 3. Mitigations including administrative physical controls

Imagine you need to protect this sensor from this specific attack and in reality the attacker may not be able to place its long probe right above your sensor's long probe to achieve maximum coupling.

One protection method often used is simple administrative physical controls by designating a no-access area around the sensor you want to protect. That is, the attacker may not be able to perform this attack if it cannot physically get close to your sensors.

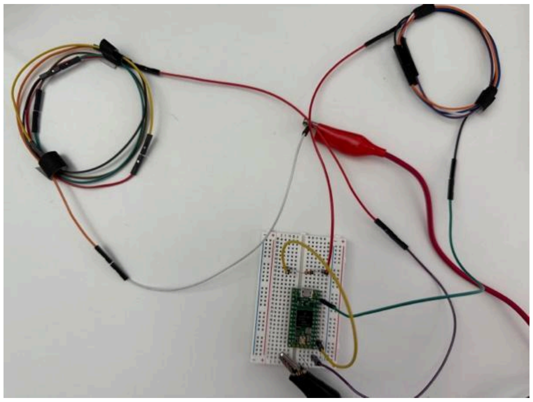


Fig. 6. Setup for demonstrating administrative physical control

To demonstrate this, move the two long probes away from each other. You can keep a distance of about 10 cm between them similar to Fig. 6. Still use a 15 MHz injection signal to make the results comparable to problem 1 and 2. Now turn your IEMI injection on and run Python Script to measure the voltages again. Fig. 7. shows what I got. The variation range is smaller than the strongest attack case in problem 2, but still larger than the no-attack case in problem 1.

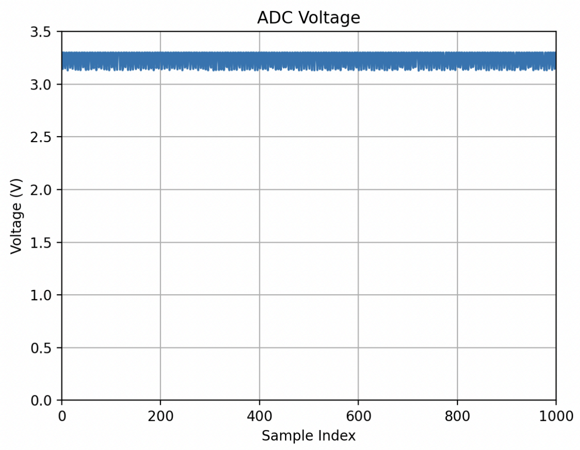


Fig. 7. IEMI ON, weak coupling.

Question 3 (2 pts):

- Submit a screenshot similar to Fig. 7 when the IEMI is on but the two long probes are parted away.
- What are the min, max, and average in this case?

Question 4 (0.5 pts):

- If you are an attacker, what methods can you think of that can potentially compensate for the loss of your attack effectiveness in the face of such an administrative control that results in long attack distances? Assume you have sufficient resources. There is at least one obvious correct answer.

Question 5 (0.5 pts):

- If you are a defender, what other protection schemes can you think of from the sensor design perspective that may also reduce the effectiveness of this attack, i.e., reduce the variation? Assume you have sufficient resources. There is at least one obvious correct answer.