The Skimmer Slayers

ATM Fraud Detector

Samuel Adames, James David, AJ DiSimone, Anahi Pineda

A card that can be inserted into an ATM and tells you whether there is a credit card skimmer attached to it or not. The card would have an app tied to it, where members with the card can upload and report the status of ATMs that were checked in different locations. Members without the card cannot upload data, but can view posts made by members with the card by possibly paying a small fee to access the information (would also be able to have discussions on forums about different ATMs, make suggestions, etc.).

Problem Statement

Card skimmers are devices that are used as a false front on an ATM or general point-of-sale (PoS) terminal. These skimmers read and record the information on the card's magnetic stripe, and the details recorded can either be downloaded or wirelessly transferred to the person who originally attached the skimmer. Some skimmers will also include spy cameras to capture videos of people typing their PIN numbers or even an additional false front on the keypad, which would capture PIN data as well. These skimmers are often difficult to notice by the average person because the skimmers are usually fitted to the original card reader, which is likely why cases of card skimming have been on the rise.

Figure 1: Example of Credit Card Skimmer

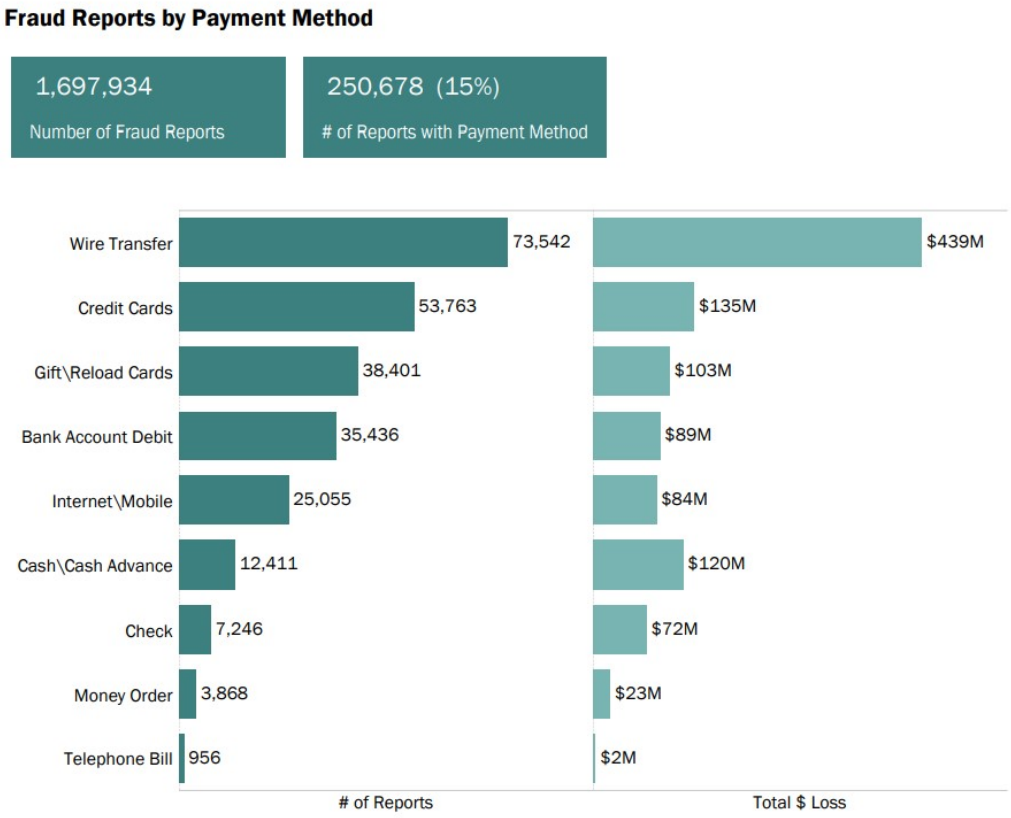

Figure 2: Fraud Types Reported to the FTC in 2019 and Corresponding Dollar Loss Amounts

The Fair Isaac Corporation (FICO) reported that card skimming fraud has grown by over 700% in the first half of 2022. Because of this, we see that card skimming is still an ever-growing problem that should be addressed as everyone is vulnerable to falling victim to this type of fraud. We decided to focus on building a credit card skimmer detector that will help warn a user of whether an ATM is “clean” in the sense that it does not detect more than one card reader through the number of magnetic stripe heads. Our product would be mainly targeted towards people who own credit and/or debit cards and often use ATMs as they are likely to find this product convenient in their everyday lives.

Objectives, Goals, & Requirements

Our main objective is to design a PCB (“Skimmer Slayer”) with similar dimensions to that of a regular credit card, and will be inserted into ATMs and general PoS readers to notify users whether a second card reader (the skimmer, in this case) is detected. If the PCB detects a second reader, it will notify the user of it through the use of a red LED, for example.

We would also want to create a companion app to the PCB that is designed. Through this app, we would encourage users with access to the “Skimmer Slayer” to upload the safety status of ATMs in their area. The app would include the location of the reader they checked along with a timestamp of when it was scanned. Users who do not own the Skimmer Slayer would be able to use this app to see what ATMs and PoS terminals have been checked, and their reported status.

A success for this project would be to have a prototype that detects a card skimmer. We would test this by quickly swiping a regular card reader twice and having the red LED we mentioned earlier light up to signify that there is likely a skimmer on the reader. Though we would need the PCB to first work before focusing on the development of the app, some progress to the app separate from the hardware could be considered the start of some success in regard to the software aspect of it. We would also consider a working MagSpoof prototype a success as it would allow us to better understand magnetic stripes and general concepts of electromagnetism that we need to be successful with our main project. If we do not get a working prototype in regard to the PCB and its design, then we would consider that to be a failure. However, if different versions of the PCB allow us to grow our knowledge and understanding of skimmers and magnetic stripes, then these versions would not necessarily be an entire failure. Lack of any progress toward the app itself would also be considered a failure to us.

Some design constraints to the card we design involve the dimensions of a typical card reader in regard to the thickness, length, and width of the reader. The PCB itself will need to be able to fit into these readers, so it must follow the magnetic stripe card standards we set. Any electronic components that we plan to add to the custom card (e.g., bluetooth adapter) will need to be on the opposite side of the card in order for it to fit into a reader. In regard to the app, it would be ideal for it to be compatible with android and IOS devices, however, there may be a number of difficulties that may arise when attempting to do so.

Towards the end of the semester, we are also looking at additional constraints involving available funds. We have used over half of our budget on the Hunter Cat as well as the components used to assemble the MagSpoof. Moving forward, we may need to modify the existing requirements to our prototype in order to stay within the budget, and in general carefully consider what we plan to purchase in advance. If we are limited by funds available to us, we would need to try and optimize our design to find the best possible solution to our problem without spending more than we can afford.

Fall Semester

WEEK	TASK
09/26/2022	● Submit a proposal, wait to receive approval
10/3/2022	● Hardware team researches card scanning technology ● Software team researches app development
10/10/2022	● Both teams conduct research, understand how to read/measure emf
10/17/2022	● Continue research, prove we can read a card and decode it ● Begin designing the overall look of the app
10/24/2022	● Focus on designing PCB, figure out what components we want to add ● Get firebase integration working with app
10/31/2022	● Look into magspoof ● Try to display data from firebase on the app
11/7/2022	● Start to work on magspoof to present for fall presentation ● Attempt to get Google Maps API working on the app
11/14/2022	● Continue to put together the magspoof ● Break apart card reader and read the code ● Continue to work on putting together magspoof
11/21/2022	● Review magspoof, make changes before this date if necessary
11/28/2022	**Thanksgiving Break**
12/5/2022	**Presentation Week, Final Report Due Following Week**

Spring Semester

WEEK	TASK
02/06/2023	● Look over what we learned from the MagSpoof ● Decide on new roads to go down
02/13/2023	● Decided to move on ● ordered new sensors

02/20/2023	• Waited for sensors to arrive • Meet as group to discuss route
02/27/2023	• Parts came in • Decided to test magnetometer first • Did research into the sensor
03/06/2023	• Tried taking apart the reader to get better readings with the magnetometer • Did research on code that went along with magnetometer
03/06/2023	• More work with the Magnetometer • Research calibration • Research magnetic shielding to improve sensing capabilities
03/06/2023	• Final attempts to work with the magnetometer • Gave up on magnetic shielding as it didn't apply to us
03/13/2023	• Look into other sensors • Decided on current sensor • Looked into current sensor
03/22/2023	• Ordered current sensor, waited for it to arrive • Continue to research sensor
03/29/2023	• Set up current sensor with card reader • Tested current from card reader
04/03/2023	• Took apart other reader to attach current sensor • Found similar results so brainstormed what else to test
04/10/2023	• Hooked up HunterCat to current sensor • Started PCB work • Met with Dr. Martin on PCB design
04/17/2023	• Worked more on PCB • Started work on poster
04/24/2023	• Continued work on poster • Continued work on PCB
05/01/2023	• Finished Poster and had Research Day • Continued work on PCB to try to have it for presentation
05/08/2023	• Worked on Presentation • Finalized any work • Presented final presentation

05/15/2023	• Worked on and finalized Spring Report

Approach & Design

Fall

Our approach and design throughout this semester involved doing extensive research into how credit cards, readers, and writers worked to help us build a base of our understanding for magstripes and card readers. Some of the research about magstripes included the different ISOs which define different aspects of ID cards. One of these was ISO7810 which defines the physical characteristics for ID cards. This standard was particularly helpful because it defined the physical dimensions our device would have to follow since it would need to be inserted into PoS and ATMs. Another set of standards we looked into fell in the range of ISO7811-1 through 7811-9 which defines the recording techniques for ID cards, within this range of standards we only looked at two: ISO7811-4 and ISO7811-6. ISO7811-4 helped us understand the location of Tracks 1 and 2 on the card. ISO7811-6 helped us understand the coercivity of all banking cards and how the encoded data is structured within the tracks. The coercivity of a card refers to the magnetic material's resistance to becoming demagnetized so a high coercivity and low coercivity represent different standards of card durability and security.

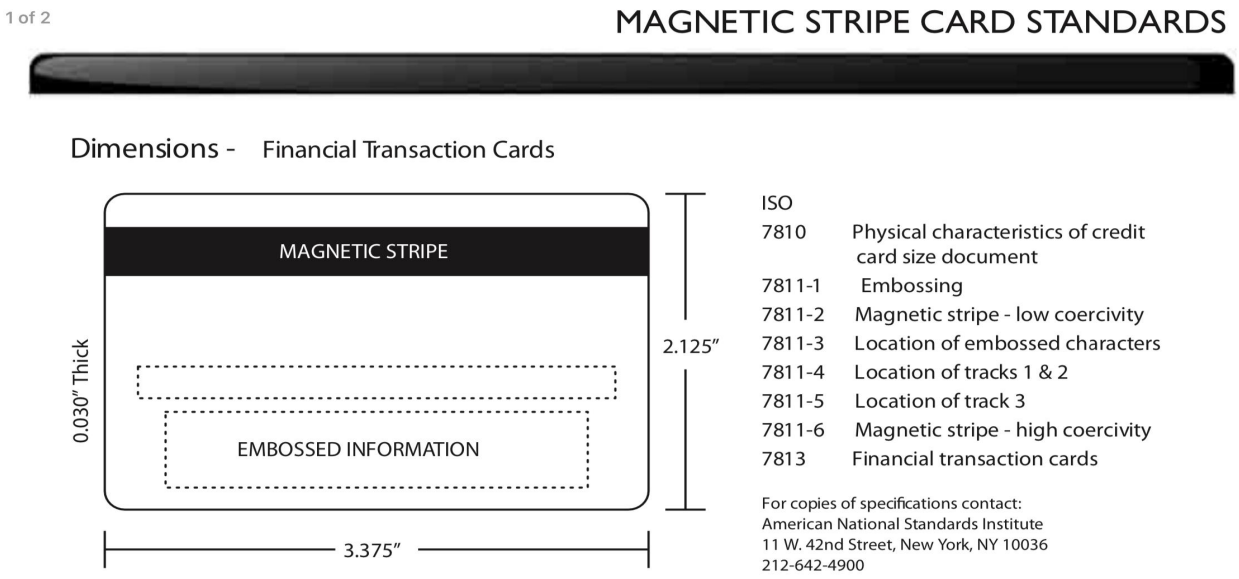

Figure 3: Magnetic Stripe Card Standards

- Figure 1 is a visual for how the ISO standards define how a magstripe card should look like, with all dimensions and locations of tracks clearly defined.

In addition to our main research focus, we dedicated a significant portion of our project to testing and experimenting with a card reader, aiming to gain insights into its functionality at a fundamental level. To accomplish this, we disassembled the card reader, allowing us to examine its internal components and understand the process by which the magnetic head reads the information encoded on the magnetic stripe as it is swiped.

To further deepen our understanding, we utilized another card reader/writer to interact with multiple cards. This hands-on approach enabled us to observe firsthand how data is structured and formatted within the various tracks of the magnetic stripe. By reading and writing to different cards, we were able to examine the specific layout and formatting of both Track 1 and Track 2, which are integral components of the magnetic stripe data.

Understanding the intricacies of how data is organized within these tracks is crucial for comprehending the functionality of the card reader and the underlying principles of card data transmission. By delving into the technical aspects of the card reader and familiarizing ourselves with the data structures, we were able to gain valuable insights that informed our development and analysis throughout the project. This hands-on experimentation not only enhanced our understanding of card reader technology but also equipped us with practical knowledge that contributed to the overall depth and accuracy of our research findings.

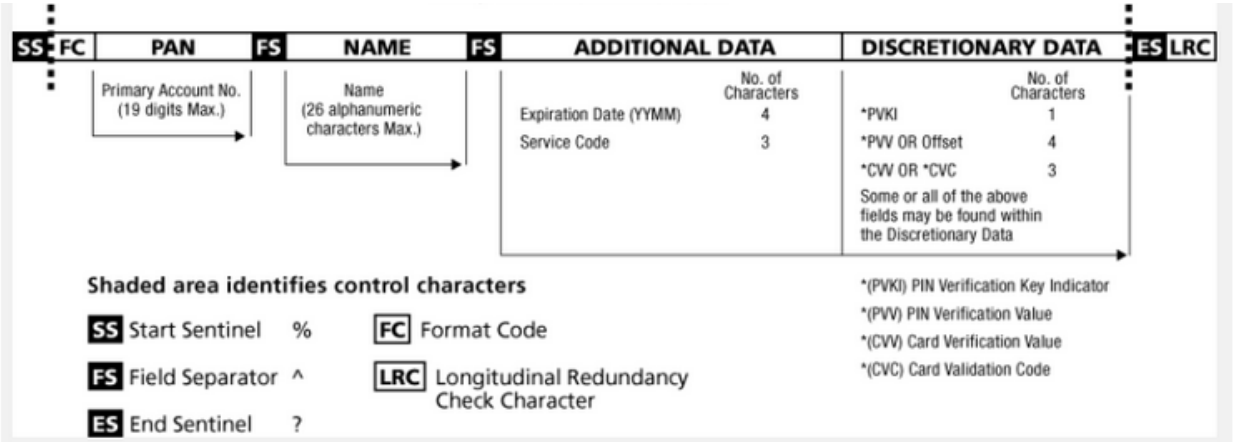

Figure 4: Track 1 Card Data Format

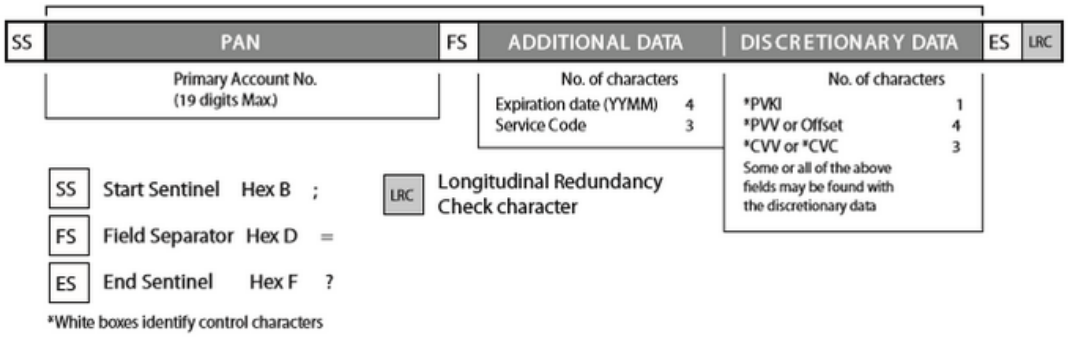

Figure 5: Track 2 Card Data Format

Most, if not all banking institutions use these two tracks to place all the information that they need. Information redundancy is built on a magnetic stripe, so if the first track is damaged, the second track can carry enough information to use the credit card to make purchases. Track 3 is not used due to the fact that it was originally created with the intention of using it for when ATMs were offline and people needed to use it, but nowadays it is required that they always remain online to use it, therefore rendering the track useless.

While doing research this semester we found our main competitor whose device contains most of the functionalities we want our device to have. The Hunter Cat is a device currently produced by Electronic Cats. The device can detect a skimmer on ATMs and PoS devices without risking your real data. It does this by detecting the number of magnetic stripe heads. We ordered the Hunter Cat and tested it on ATMs and multiple basic card readers. When testing it we found that it was not long enough to detect the reader on some ATMs, so it would not give any indication of it working with the LED lights. When we tested it on the card reader, however, we did get some good results. When it detected one reader the green LED would light up, when it detected two readers the red LED would light up, and when it was unsure about the reading a yellow LED lit up. The way we went about detecting two heads with the hunter cat was by swiping it in under a second with two readers.

Figure 6: Hunter Cat by Electronic Cats

We reached out to Electronic Cats, as well as Salvador Mendoza, but only received a response from Mendoza. Mendoza was able to give us some helpful advice on what direction we should take as a team, but nothing specific about the Hunter Cat given that he is no longer involved with Hunter Cat and stated that it was now a private project. Another device we researched and built as part of our approach to better understand card reader technology was the magspoof. The magspoof is a card emulator developed by Sammy Kamkar which helped us understand concepts of electromagnetism and provided us with a better understanding of how magnetic stripes work.

The magspoof is a wireless credit card spoofer originally designed by Samy Kamkar that allows you to store your cards in one device. It emulates a magnetic stripe by quickly changing the polarization of an electromagnet, producing a magnetic field similar to that of a normal magnetic stripe as if it's being swiped through a card reader. It supports all 3 magnetic strip tracks, supports tracks 1 and 2 simultaneously and works on traditional magstripe readers wirelessly (no NFC/RFID required). This type of device allowed us to perform research in other areas of magnetic stripes and helped us make substantial progress in our design for our main credit card skimmer detector.

Components Used	Purpose
Atmel ATtiny85	Microcontroller to store all of the magstripe data
L293D H-Bridge	Motor driver to drive the electromagnet
24 AWG Magnet Wire	Produce the electromagnetic field
3.7V LiPo Battery	Power the device
Capacitor	Store electrical energy for when needed
LED	Signal when information is transmitted
Resistor	Avoid burning out LED
Momentary Switch	Initiate electromagnet
Protoboard	Solder everything together

Here we can see all the pieces that were required in order to build and put together the magspoof, with each a little description of what each element does for the final design.

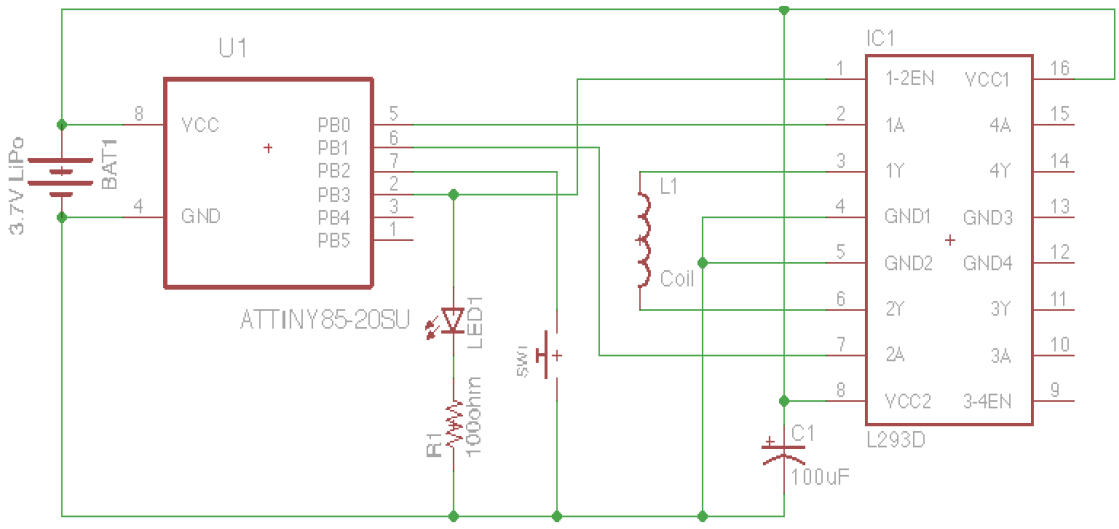

Figure 7: Magspoof Schematic

And in this picture, we have the schematic of how the magspoof is put together and how everything flows. To give a brief explanation, when the button is pressed, current will flow to the electromagnetic coil wrapped around the pcb board that is given from the L293D motor chip, and will emulate a magnetic field that is controlled by the ATtiny85 chip, in order to give off the correct polarity in order for the card reader to properly get the credit card information stored. When this process completes, the LED will light up in order to tell the user that everything went through correctly.

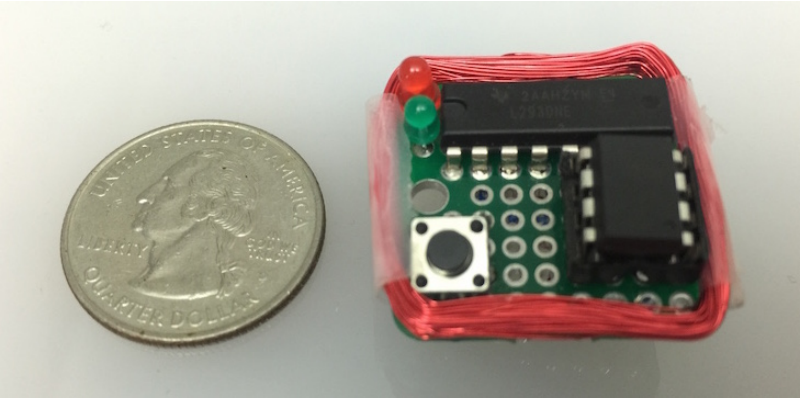

Figure 8: Magspoof Design

Regarding the magspoof design, our aim was to replicate the original design created by Samy Kamkar. While there were some minor add-ons in his design, such as an extra LED and additional features on the back side, we made the decision not to include them in our version. These add-ons were not present in other hardware and software schematics we referenced, leading us to exclude them from our magspoof design.

In terms of the software aspect, our magspoof utilizes a variety of features. The software is primarily written in C and focuses on sending tracks stored in memory. This process is executed rapidly, allowing for the transmission of one to three tracks. Since not all cards utilize all three tracks defined by the ISO standards, the software is flexible enough to handle different track configurations. Additionally, the software is capable of simultaneously sending tracks 1 and 2, with track 2 reversed. This manipulation tricks the card reader into perceiving a quick swipe, providing the MagSpoof with extended time to transmit the track data effectively.

Moreover, during this semester, we laid the foundation for our application using Dart and Flutter. The application is being developed for the Android platform and is intended to integrate seamlessly with our skimming detector device. Our goal is to enable users to share the status of ATMs checked by our device through this application. By allowing users to provide updates on the cleanliness and safety of ATMs, we aim to create a collaborative platform that enhances awareness and helps protect individuals from falling victim to card skimming fraud.

Spring

Our approach and design throughout this semester involved the testing of different sensors. We researched a list of potential sensors to use to detect the magnetic field produced when a card is inserted into an ATM. After some thorough research we decided to use a magnetometer as our first sensor.

Sensors:

LIS2MDL

A magnetometer is a device that is used to measure the magnetic field for the three physical axes (x, y, z). The specific magnetometer was the LIS2MDL sensor. This sensor had a high sensitivity making it ideal since we needed to detect small changes in the magnetic field. On top of having high sensitivity, it had a wide range of measurement, with a dynamic range of ±50 gauss. The sensor also had very low power consumption and it came in a small size making it even more ideal for battery-powered devices and for a good range of them.

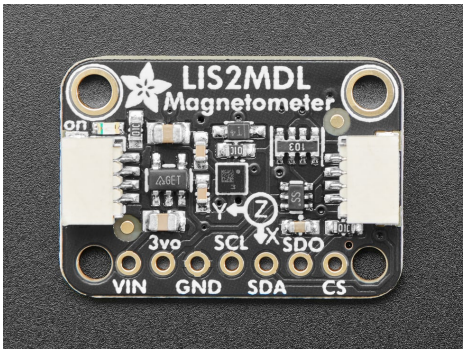

Figure 9: LIS2MDL Magnetometer

```
#include <Adafruit_LIS2MDL.h>
#include <Adafruit_Sensor.h>
#include <Wire.h>
#include <math.h>

/* Assign a unique ID to this sensor at the same time */
Adafruit_LIS2MDL lis = Adafruit_LIS2MDL();
Adafruit_LIS2MDL lis2mdl = Adafruit_LIS2MDL(12345);

/* Set the hard offsets for each axis */
float xOffset = -5.68;
float yOffset = -7.48;
float zOffset = 19.34;

void setup(void) {
  Serial.begin(115200);
  while (!Serial)
    delay(10); // will pause Zero, Leonardo, etc until serial console opens

  Serial.println("LIS2MDL Magnetometer Test");
  Serial.println("");

  /* Enable auto-gain */
  lis2mdl.enableAutoRange(true);

  /* Initialise the sensor */
  if (!lis2mdl.begin()) {  // I2C mode
    /* There was a problem detecting the LIS2MDL ... check your connections */
    Serial.println("Ooops, no LIS2MDL detected ... Check your wiring!");
    while (1) delay(10);
  }

  /* Set the range to 8 gauss (default is 4 gauss) */
///
  /* Display some basic information on this sensor */
  lis2mdl.printSensorDetails();
}

void loop(void) {
  /* Get a new sensor event */
  sensors_event_t event;
  lis2mdl.getEvent(&event);

  /* Apply hard offsets to each axis */
  float x = event.magnetic.x - xOffset;
  float y = event.magnetic.y - yOffset;
  float z = event.magnetic.z - zOffset;
```

Figure 10: LIS2MDL Calibration Code

After conducting multiple tests, we made the decision not to proceed with the LIS2MDL for our project. The results of these tests did not meet our expectations. Despite its sensitivity, the LIS2MDL proved insufficient in detecting the magnetic field generated by swiping a card through a reader. Even after calibration, the sensor failed to accurately measure the magnetic field, rendering it ineffective for our intended purpose.

Another issue we encountered was significant electromagnetic interference from the surrounding devices such as computers and phones, despite relocating to a quieter environment. This interference further hindered the sensor's performance and contributed to inaccurate measurements.

As a last-ditch effort, we explored the option of magnetic shielding. This approach involves using a conductive barrier between the sensor and potential sources of interference to reduce electromagnetic disturbances. However, upon closer examination, we determined that implementing magnetic shielding would not align well with our overall design goals, leading us to ultimately discard this option as well.

INA169

Through further research, we found that a current sensor was a more appropriate choice than a magnetometer for measuring the change in magnetic field produced when a card is swiped through a reader. We discovered that by measuring the induced current flowing through the card reader using a current sensor, we can better gauge a threshold value to have a way to determine whether a skimmer is on an ATM or not. The current sensor we used was the INA169. It is a module that enables you to conveniently measure the direct current while providing an analog output that is relative to ground. We connected the sensor in series with our card reader and measured the differences between 1 swipe and 2 fast swipes, since we were not able to acquire an actual skimmer.

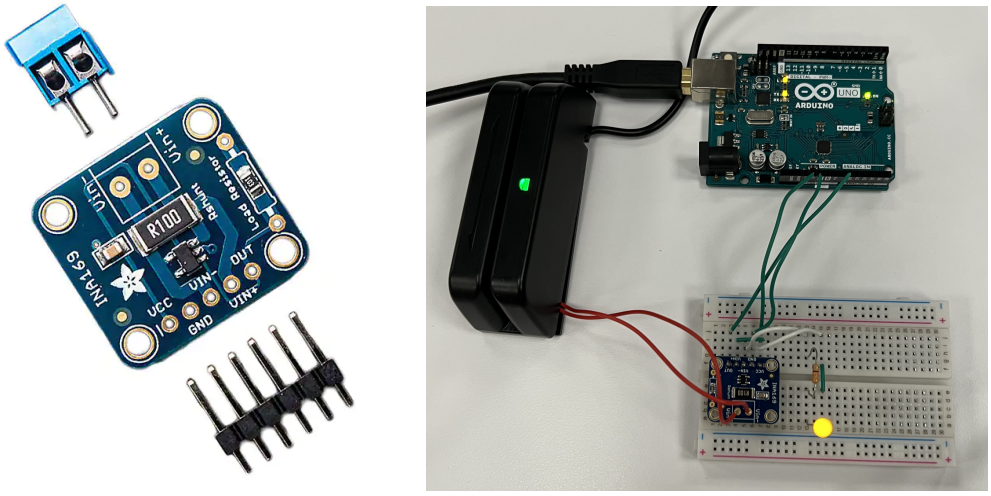

Figure 11: INA169 Connected in Series with Reader

```ino
#include <Arduino.h>

// Define the analog input pin for the INA169 output
const int SENSOR_PIN = A0;

// Define the reference voltage for the ADC (5V for most Arduino boards)
const float VOLTAGE_REF = 5.0;

// Define the value of the shunt resistor (RS) in ohms
const float RS = 0.1; // Change this value according to your shunt resistor

// Define a scaling factor to make the numbers larger
const float scalingFactor = 100.0;

void setup() {
  // Initialize the serial communication at 9600 baud rate
  Serial.begin(9600);
}

void loop() {
  // Read the raw ADC value from the INA169 sensor
  int rawSensorValue = analogRead(SENSOR_PIN);

  // Remap the ADC value into a voltage number (5V reference)
  float sensorValue = (rawSensorValue * VOLTAGE_REF) / 1023.0;

  // Follow the equation given by the INA169 datasheet to
  // determine the current flowing through RS. Assume RL = 10k
  // Is = (Vout x 1k) / (RS x RL)
  float current = sensorValue / (10 * RS);

  // Multiply the current by the scaling factor
  float scaledCurrent = current * scalingFactor;

  // Output the scaled value to the serial monitor
  Serial.print(scaledCurrent, 1);
  Serial.println(" A");

  // Delay program for a few milliseconds
  delay(100);
}
```

Figure 12: INA169 Current Sensor Code

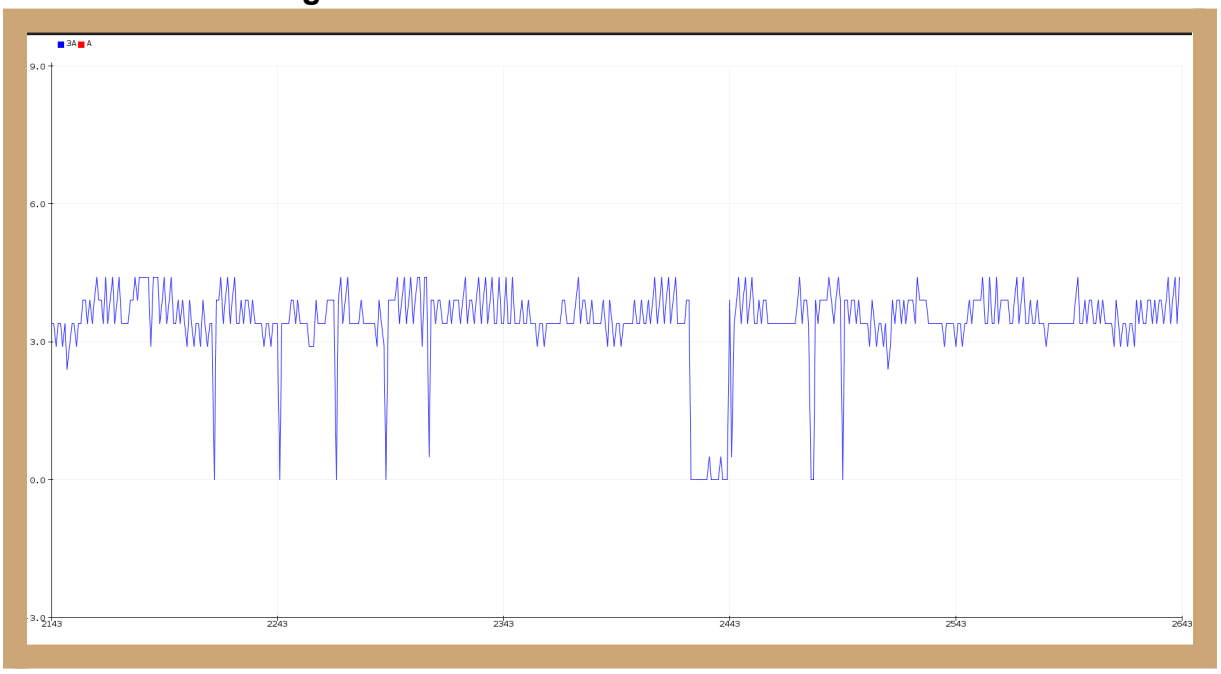

Figure 13: Serial Graph of Sensor for 1 Swipe vs 2 Swipes

Hunter Cat Current Testing

While half the group was testing the INA169 module on the card reader, the other half wanted to measure the induced current that the hunter cat was collecting from its coils as we believed that the hunter cat worked by collecting the induced current from its coils as it swiped through the solenoid in the card reader, and from there the induced current went to the analog pin on the microprocessor to be converted to a digital signal in order for the chip to read and do whatever processes it does from there.

We first connected two wires to the hunter cat, one to the analog pin where we believed the induced current was going, and one to the ground pin. From here we connected our setup to a oscilloscope in order to see the current going through and the reading was wonky as it was going all over the place and we wanted to be able to have a numerical value for current so we could theoretically set a ‘threshold value’ for the induced current (If the induced current is greater than a set threshold than your card is going through more than one card reader, aka a skimmer, and you’d have a way to detect a skimmer from the induced current).

From here we decided it was better to connect our setup to a breadboard and measure the current with the WaveForms program. We connected everything together and swiped the hunter cat through a card reader to see what current came up, and we did 1 and 2 fast swipes to compare a ‘clean’ card reader vs a ‘skimmed’ card reader. We also took note of which color the hunter cat blinked to see what it detected.

Figure 14: Graph that shows induced current in hunter cat, no swipes done however still has steady current

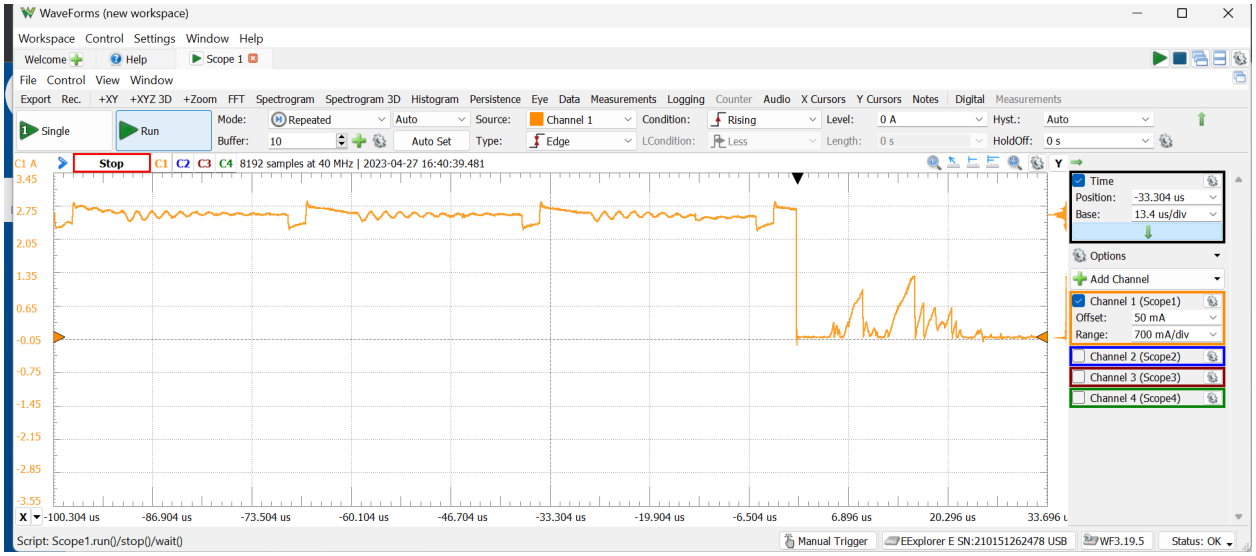

Figure 15: Graph that shows induced current in hunter cat for 1 swipe with a green light blink

Figure 16: Graph that shows induced current in hunter cat for 2 swipes with a red light blink

Now before anything, we realized late that there was an error in the setup of these tests as the induced current should not be 3 amps… at all, but there is still data that can be utilized in these graphs where the amplitude of the current doesn't actually matter, unlike we thought.

From these graphs, we see that there is always a steady current coming in and when a card is swiped, the current drops to 0 for a second. Now we originally thought that the current would be close to 0 amps to start and spike when it goes through a card reader, and that the current spike would be greater if there was a skimmer attached.

What we learned here is that it is kind of the opposite way as there is always a higher current and it drops instead of spikes, but the same principles apply.

When looking at the graphs, it is clear to see when a card is swiped through a card reader, as the current drops close to 0 quickly before going back up, and even when the card is quickly swiped twice to emulate what a skimmer would look like, you can see two clear distinct drops. This is good because this is where our 'threshold' could be. What I mean here is that instead of going for a threshold that is based on the amplitude of the current, we can set a threshold that takes notes of how many drops in current there are when a card is swiped and if there is more than one drop, that could be the way you detect a skimmer.

One last thing to also note here is that again, we don't have a skimmer to test so we have to extrapolate our data. The evidence that backs all of our theory up on this test, is the color blinks on the hunter cat as we tested it. When we tested the induced current for one swipe on the hunter cat, it blinked back a green light to us, indicating that the device believed it only went through one clean card reader. When we swiped it twice, we had some issues on what color popped up, but the graph above shows 2 swipes with a red light appearing, meaning the device believed that it went through a card reader with a skimmer on it.

PCB and Circuit Design

After testing and deciding on measuring the induced current rather than the electromagnetic field, we ultimately came to the conclusion that it was best to reverse engineer the hunter cat. So, why did we choose to reverse engineer the HunterCat? First and foremost, its functionalities aligned perfectly with our project goals. This was a device that already did exactly what we wanted our project to accomplish. Secondly, we found it to be a cost-effective approach. Rather than keep spending our budget on a range of sensors and testing, we were able to focus our resources on a single, proven design. Lastly, reverse engineering allowed us to customize and improve upon the HunterCat. We would then potentially take it a step further, planning to extend its length and implementing an ATM database through an app. This way, users can provide updates on the status of the ATM.

Getting started, we began with the task of taking measurements. We had to ensure the dimensions of the metal pieces on the HunterCat were captured accurately for our PCB design. We also measured the thickness of a typical credit card to ensure our PCB would fit seamlessly in similar slots. Finally, we identified the exact components on the HunterCat, laying the groundwork for our own design. The exact components included: a capacitor, (3) LEDs, programming cable (TC2030), (3) 3.3k resistors, push button, battery holder (CR2032), (4) metal pieces, and finally the SAMD11C14-pin where all the magic happened.

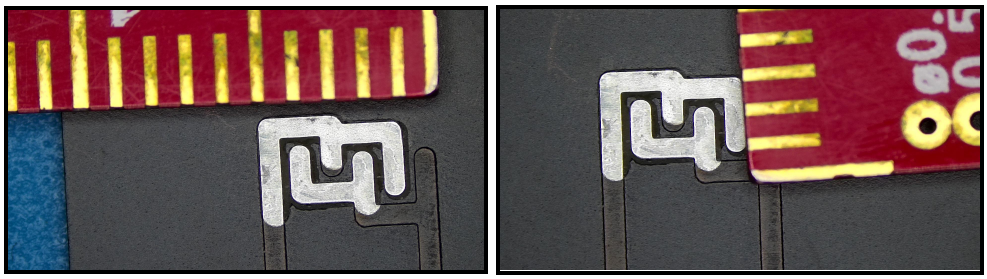

Figure 17: Measurements of Metal Pieces

In the schematic design phase, we strategically pieced together our reverse-engineered version of the HunterCat using KiCad, a tool for PCB design. This schematic incorporates all necessary components, along with custom-made metal pieces that we created in the footprint editor. These metal pieces play a key role in our design; the upper pieces interface with the analog inputs while the lower pieces connect to the ground. As the device operates, an induced current travels through these metal pieces and is directed towards the analog inputs. At this juncture, the microcontroller's Analog-to-Digital Converter (ADC) steps in, transforming the analog input into a digital signal. Following this conversion, further operations are executed to ascertain the presence of a skimmer. This precise and efficient process forms the core of our design.

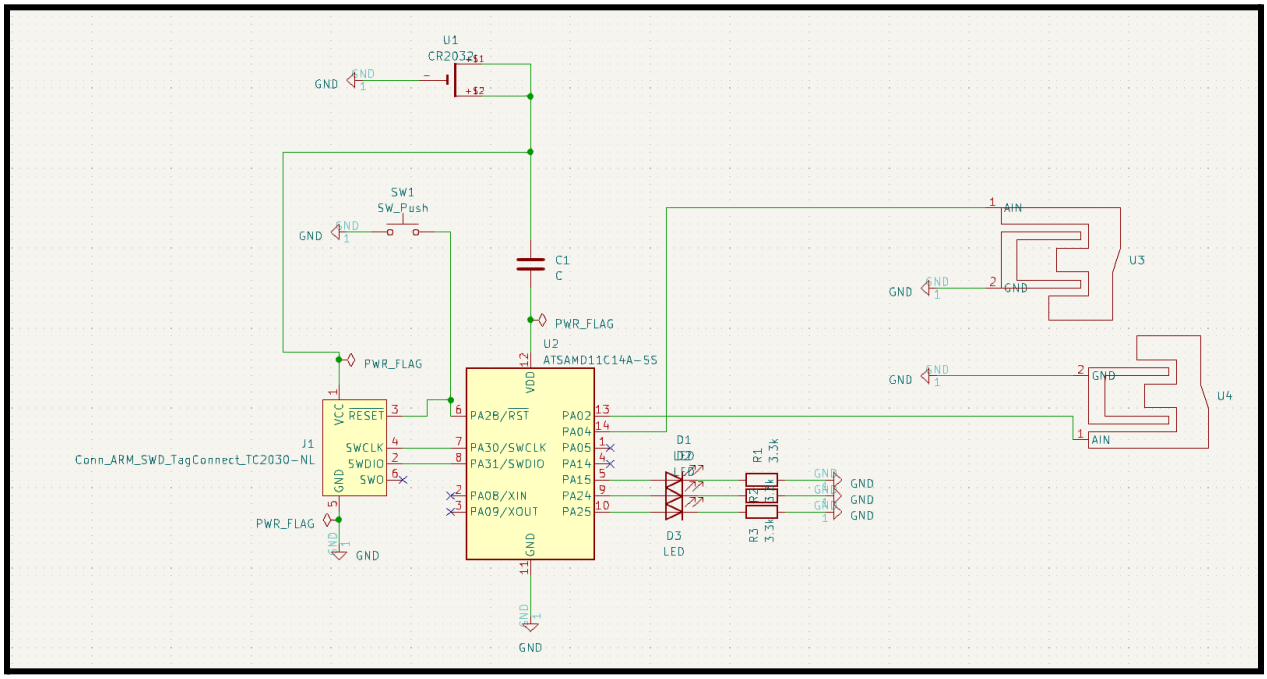

Figure 18: PCB Schematic

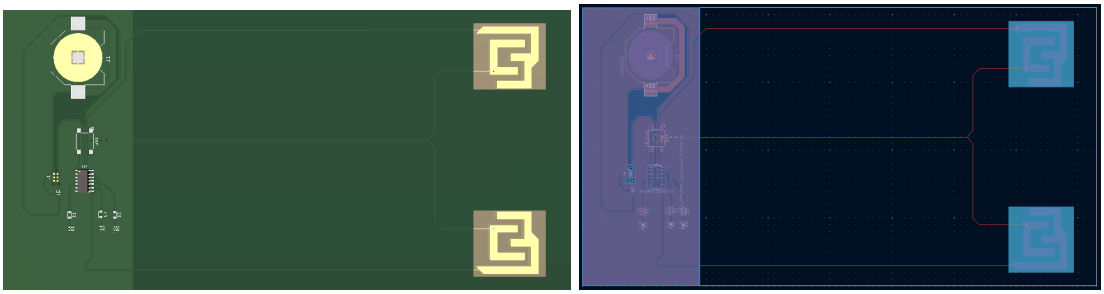

Figure 19: 3D View of Design and Board Editor

Challenges

- Developing the app in a timely manner
- To our knowledge, the Hunter Cat is the only product on the market that can help us further our research and development, and it has been hard to use as reference or guide given the private nature of the project by Electronic Cats
- Getting MagSpoof to work and understand why it does not work
- Understanding the software aspect of the magspoof without having a proper prototype working
- Not being able to buy a skimmer
    - Because of this alone, a lot of the data and results we were getting had to be extrapolated and even almost assumed. We still found good data and believe that what we found would still hold true for a skimmer, but still are not certain.
- Sensitivity issues with LIS2MDL magnetometer module

Safety Issues

Overall, safety concerns in this project were minimal. However, there was one aspect that could be deemed potentially unsafe. We needed to switch the ports of a live battery, requiring careful handling to avoid any electrical shocks. To mitigate this risk, we proceeded cautiously, ensuring that each wire was unsoldered individually, preventing any inadvertent contact and potential shocks to the person working on it. Thankfully, this process was executed successfully without any incidents of electrical shock, and the port switch was completed as intended. Aside from this specific situation, no other safety issues were observed throughout the project.

Project Results, Results of Component and Sub-System Testing

For our results, we will go over how building the MagSpoof went for us. We ordered all parts that were recommended by the developer and assembled it as best as we could according to the schematic. We had to make some adjustments however, since our protoboard was a bit bigger than the developers, we had to wrap the coil around the board around twice more than the original, and the parts were in slightly different places. When trying to test the MagSpoof we built, the test was not successful.

We saw some voltages on the board, but nothing substantial. After subsequent tests, there were no more voltage detections at all, leading us to believe that a short had occurred somewhere in the circuit.

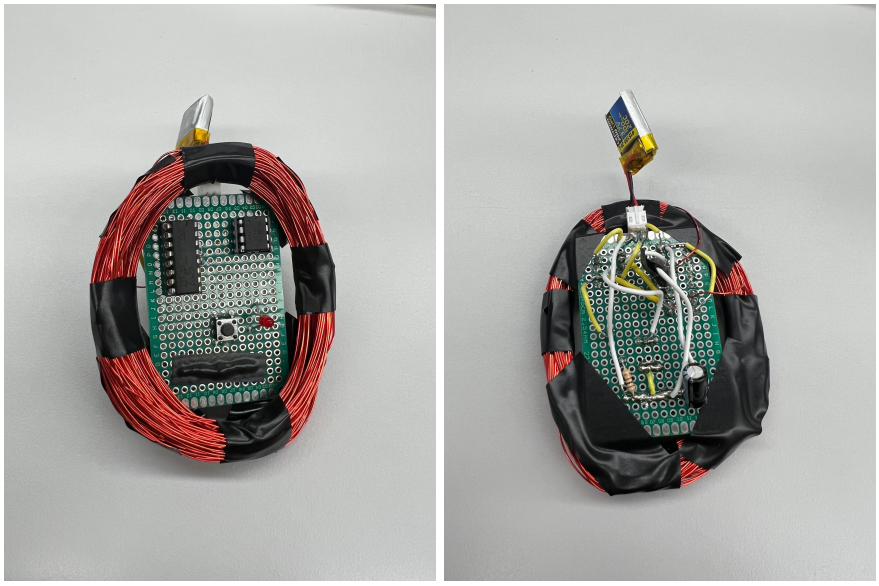

Figure 20: MagSpoof Assemblage

While we made significant progress in our project, aimed at improving upon the HunterCat's design, we unfortunately were unable to complete the printing of the board within our given timeframe. This prevented us from fully realizing our vision for an enhanced HunterCat. Despite this setback, the journey proved to be a fulfilling and educational one.

Our testing allowed us to delve deeper into complex concepts such as electromagnetism, skimmers, and the operation and formatting of magnetic stripes. These insights, though theoretical, hold practical implications and will undeniably prove valuable for the future. Constraints did arise during the course of our work, notably, the inability to procure a skimmer. This necessitated a workaround involving simulated skimmer swipes, which could have introduced some inaccuracies in our measurements. We also looked into the development of a companion application intended to pair with our improved skimmer detector. While we made initial progress, the time-intensive nature of sensor testing and troubleshooting meant that this aspect of the project did not progress as far as we would have liked. Reflecting on our project management, we acknowledge there were areas where we could have improved, particularly in terms of time management. Despite the challenges and constraints, we remain proud of our efforts and the knowledge we've gained through this process. This experience has imparted valuable lessons that will inform our approach to future projects.

Lessons Learned

Throughout these past two semesters, there were a number of lessons learned regarding teamwork, communication, and project management. Though everyone in the

team was dedicated to making the project a success, we could have made better progress with more effective communication in place. One key lesson that everyone in the group can agree on is the importance of having clearly defined roles from the beginning, and carrying those roles throughout the entirety of the project. In the beginning of the fall semester, we had roles assigned for certain parts of the project, but as time went on, we fell out of those roles and would occasionally work on tasks not necessarily within the scope of our respective roles. Tasks began to be completed without clear-cut roles, which would unfortunately lead to confusion and inefficiency. Sometimes the work we completed individually would overlap while other tasks lacked significant progress. In hindsight, we should have addressed this immediately to avoid letting it drag on. This would have given some clearer structure to the project, which would have ensured a more balanced workload and allowed for more progress to have been made overall.

Another area where we realized improvements could be made was communication. We would communicate often, but not necessarily in the best way. We made the mistake of assuming that everyone was on the same page and this caused some misunderstandings and setbacks in the project. Throughout the weeks, we should have established regular check-ins between us where we would consistently share progress updates with each other. This would have led to more transparency between us and the progress of the project.

We also acknowledge that we learned the hard way about the necessity of setting realistic expectations and deadlines, as well as managing our time effectively. There was a tendency in our team to underestimate the time it would take to complete certain tasks, which would lead to work being completed on a time crunch when it wasn't necessary had we managed our time better. The quality of our work overall would have been a lot better had we managed ourselves as a group accordingly. For the future, we recognize that we should focus on creating a more realistic project timeline and consider unexpected challenges that may arise.

Reflecting on the project, the lessons we learned were not only valuable for us as students in senior design, but also for any team project. And although our own project and results were less than what they could have been, the lessons learned will undoubtedly make us more efficient and productive in future team projects. The course itself has also allowed us to learn these valuable skills that we will have to use in future work. Much like the real world, there needs to be teamwork, communication, and proper project management to be successful. As a team, we've learned a lot about this, and we feel as though the experience in our soft skills as well as our experience with the design process has helped prepare us for becoming professional engineers.

Recommended Future Work

The nature of this project has potential for future continuation. While our focus was primarily on magstripe payments, it is important to recognize that this form of payment is gradually diminishing in popularity with the emergence of new payment

methods such as RFID tap-to-go, mobile wallets like Apple Pay and Venmo, and the increasing prevalence of online transactions. While magstripe technology remains relevant, its usage is expected to decline over time. Therefore, if this project were to be revisited or a similar endeavor pursued, we strongly recommend expanding the scope to accommodate different payment types. Embracing the shift towards online transactions would be particularly advantageous, considering the growing prominence of the digital landscape in our society.

Another valuable suggestion for future work on a project like this involves obtaining an actual skimmer device to conduct authentic tests and collect accurate data. As mentioned earlier, due to the unavailability of a skimmer during our project, we had to rely on extrapolation and assumptions to compensate for the lack of concrete data. To avoid such limitations, we propose that a future team explores the possibility of acquiring a skimmer early on in their project. This could potentially be facilitated with the support of the university or other relevant resources, as it would greatly enhance the quality and reliability of the research conducted.

Additionally, we advise that a future team undertaking this project invests time in thoroughly understanding card electromagnetics right from the beginning. By gaining a comprehensive understanding of this subject matter at an early stage, it becomes feasible to build prototypes and conduct experiments during the initial semester. In our case, constructing the magspoof in the first semester was risky, for lack of better word. While it provided valuable knowledge, unfortunately, we were unable to achieve a working prototype within the given timeframe. This setback could have potentially delayed the progress of developing the actual device. Hence, familiarizing oneself with card electromagnetics at the outset would enable a more efficient and effective timeline for the project, reducing the risk of unforeseen challenges and delays.

Project Standards

(Standards are broken down further in the approach section along with pictures to give a visual)

- ISO/IEC 7810: Defines physical characteristics for ID cards
- ISO/IEC 7811-1 through 7811-9: Standards for the recording technique for ID cards
- ISO/IEC 7813: Defines properties of financial transaction cards (e.g. credit cards)

References

- https://www.magtek.com/content/documentationfiles/d99800004.pdf
- http://sagan.gae.ucm.es/~padilla/extrawork/card-o-rama.txt
- https://en.wikipedia.org/wiki/ISO/IEC_7810
- https://en.wikipedia.org/wiki/ISO/IEC_7811
- https://en.wikipedia.org/wiki/ISO/IEC_7813
- https://github.com/samyk/magspoof
- https://d1.amobbs.com/bbs_upload782111/files_32/ourdev_576474.pdf
- https://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-42363-SAM-D11_Datasheet.pdf
- https://cdn-learn.adafruit.com/downloads/pdf/adafruit-lis2mdl-triple-axis-magnetometer.pdf

APPENDIX

Equipment used, as well as their prices can be found here:

Components Used	Cost
The Hunter Cat	$59.48
(2) Atmel ATtiny85	$10.99
(11) L293D H-Bridge	$27.35
24 AWG Magnet Wire	$20.08
(2) 3.7V LiPo Battery	$12.75
Capacitor	Taken from Evans Hall
LED	Taken from Evans Hall
Resistor	Taken from Evans Hall
(100) Momentary Switch	$8.98

(25) Protoboard	$14.49
LIS2MDL module	$5.95
INA169 Module	$9.95

In total, we have spent $170.02.