Magnetic Stripe and RFID Skimming Device with Bluetooth Functionality

Eric Smith
Eric.Smith@unh.edu
Faculty Advisor: Dr. Dean Sullivan
Department of Electrical and Computer Engineering, University of New Hampshire, Durham, NH 03824

Introduction

Goal: Design and build a multi-function device that can skim, process, and copy RFID and magnetic stripe data which can be transmitted back to a main device over Bluetooth in order to demonstrate the flaws of these data storage systems.

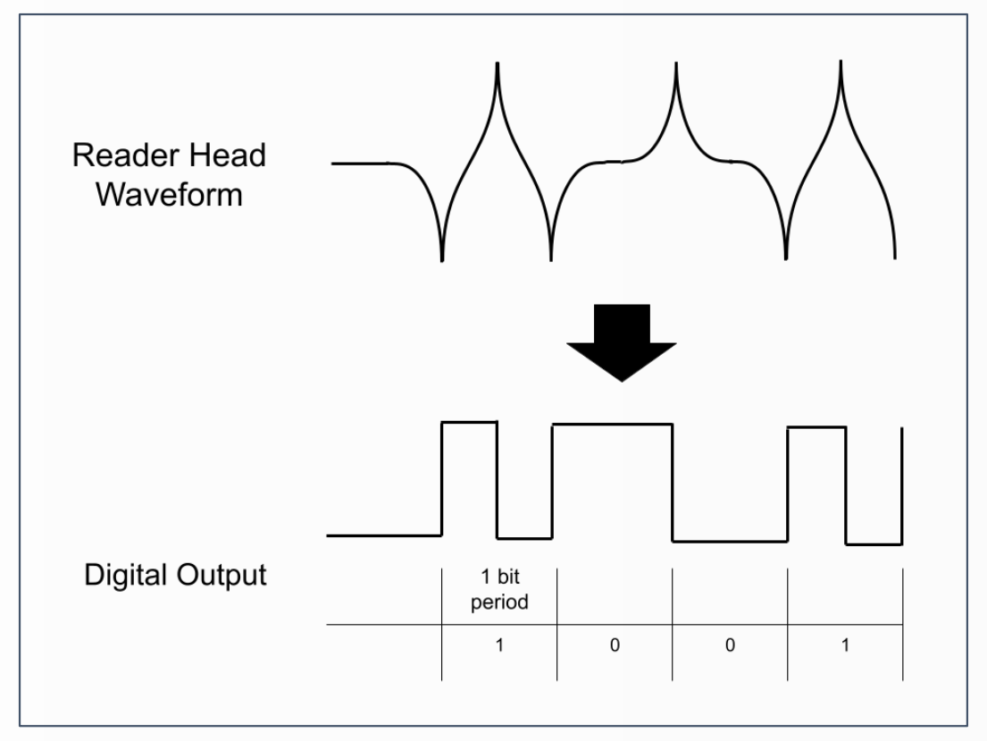
Motivation: While magnetic stripe cards are being phased out by RFID and chip cards, both RFID and magnetic stripe cards are still widely used in a variety of applications, leading to potential security flaws in these systems.

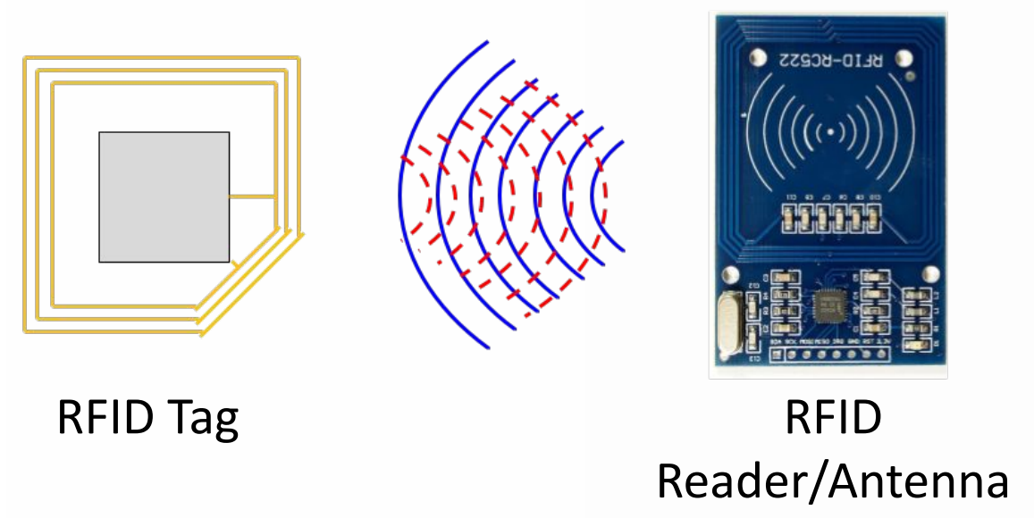
Requirements:

- RFID HF Data Skimming and Copying
- Magnetic Stripe Skimming and Copying
- Bluetooth communication and reporting to a main computer for data use (mode selection).

Background

- Cards using a magnetic stripe to store important data are still being used widely today in applications such credit, debit, or identification cards.
- The data is stored on these cards by encoding magnetic north and south poles in the strip which can be decoded as 1s or 0s as shown to the right.

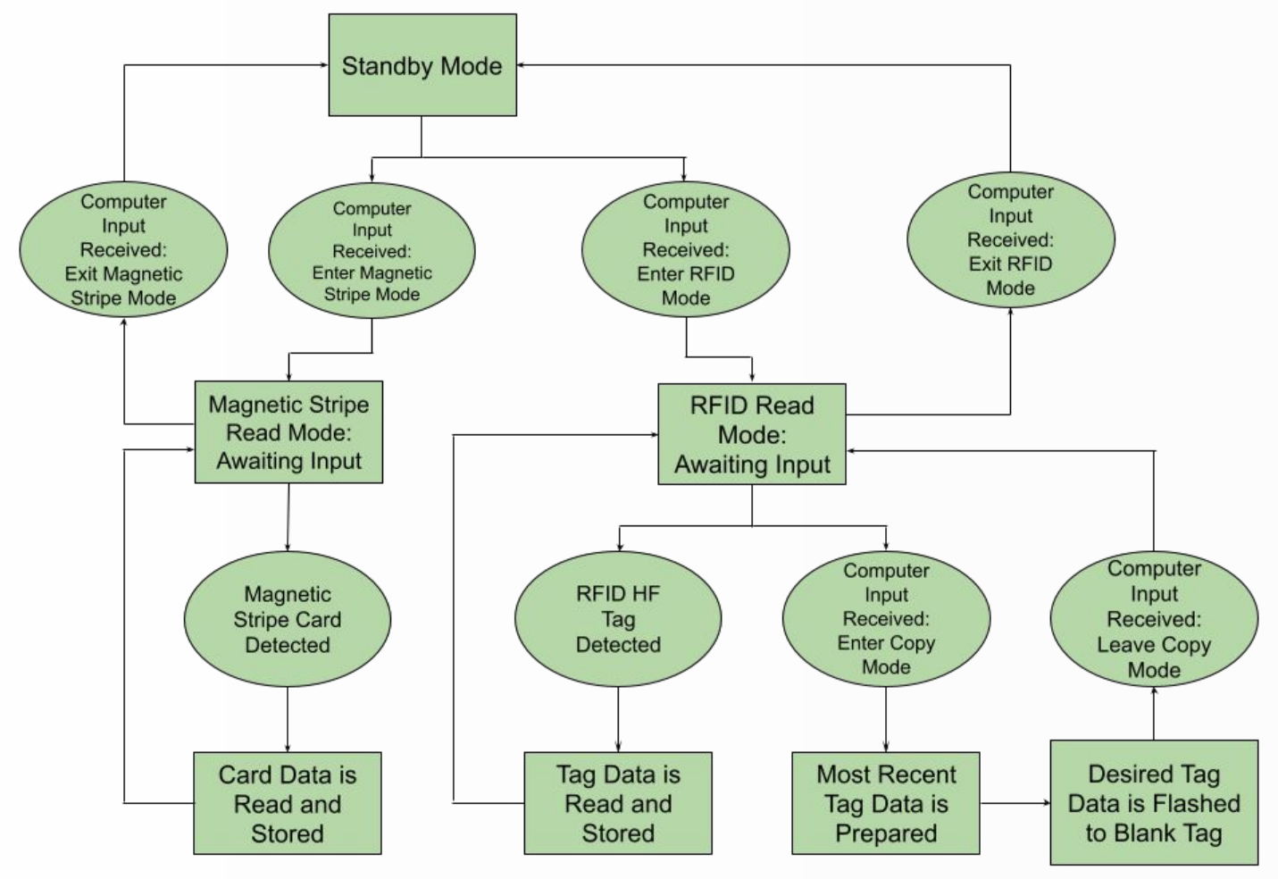




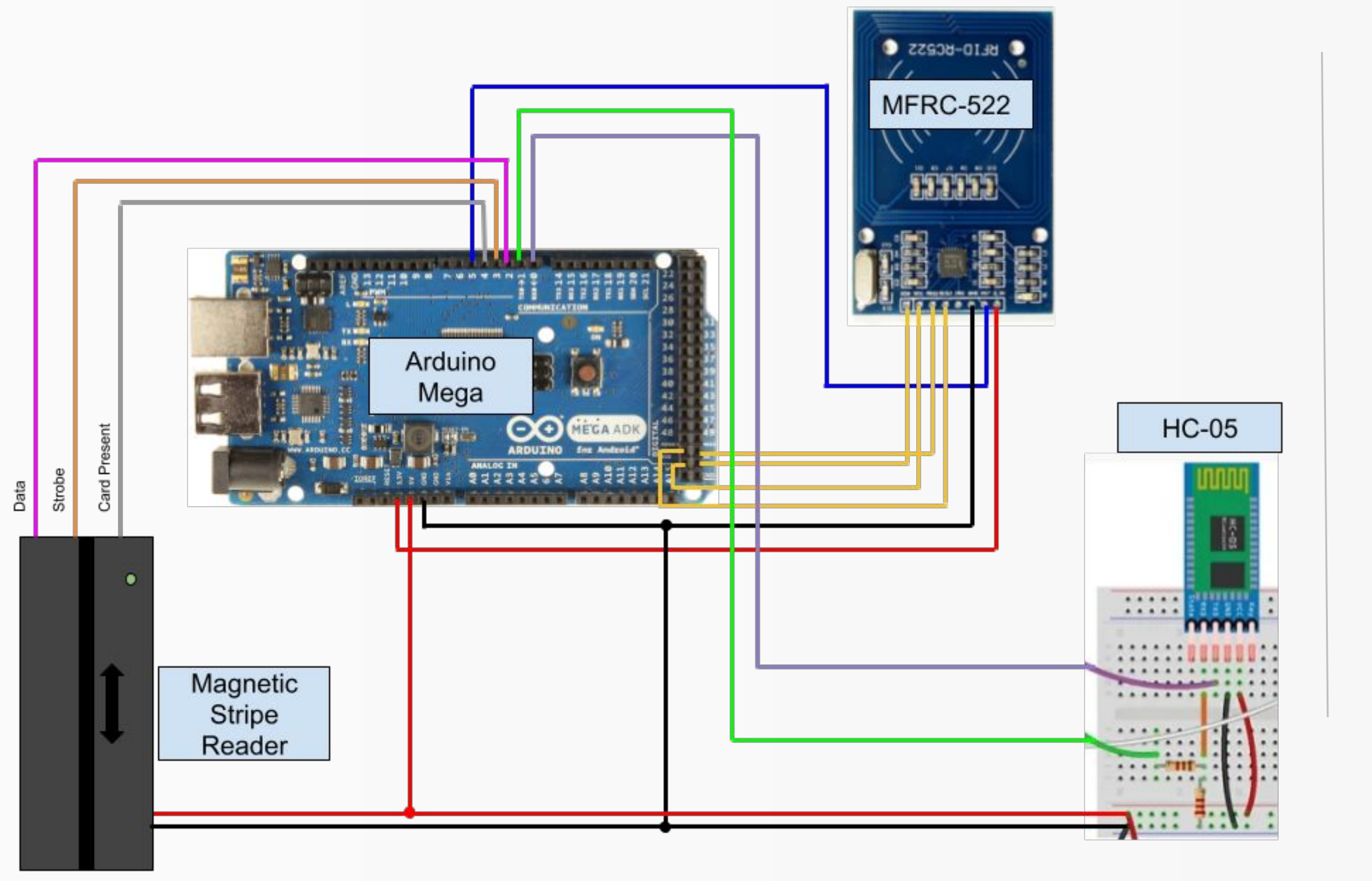
- Much like magnetic stripe technology, many payment and identification cards carry RFID, or Radio Frequency IDentification.
- In this case, data is stored on a "tag" which is connected to an antenna as shown to the left. When it receives a power up radio signal from a reader, it uses this antenna to transmit its stored data back to the reader.

Software Design

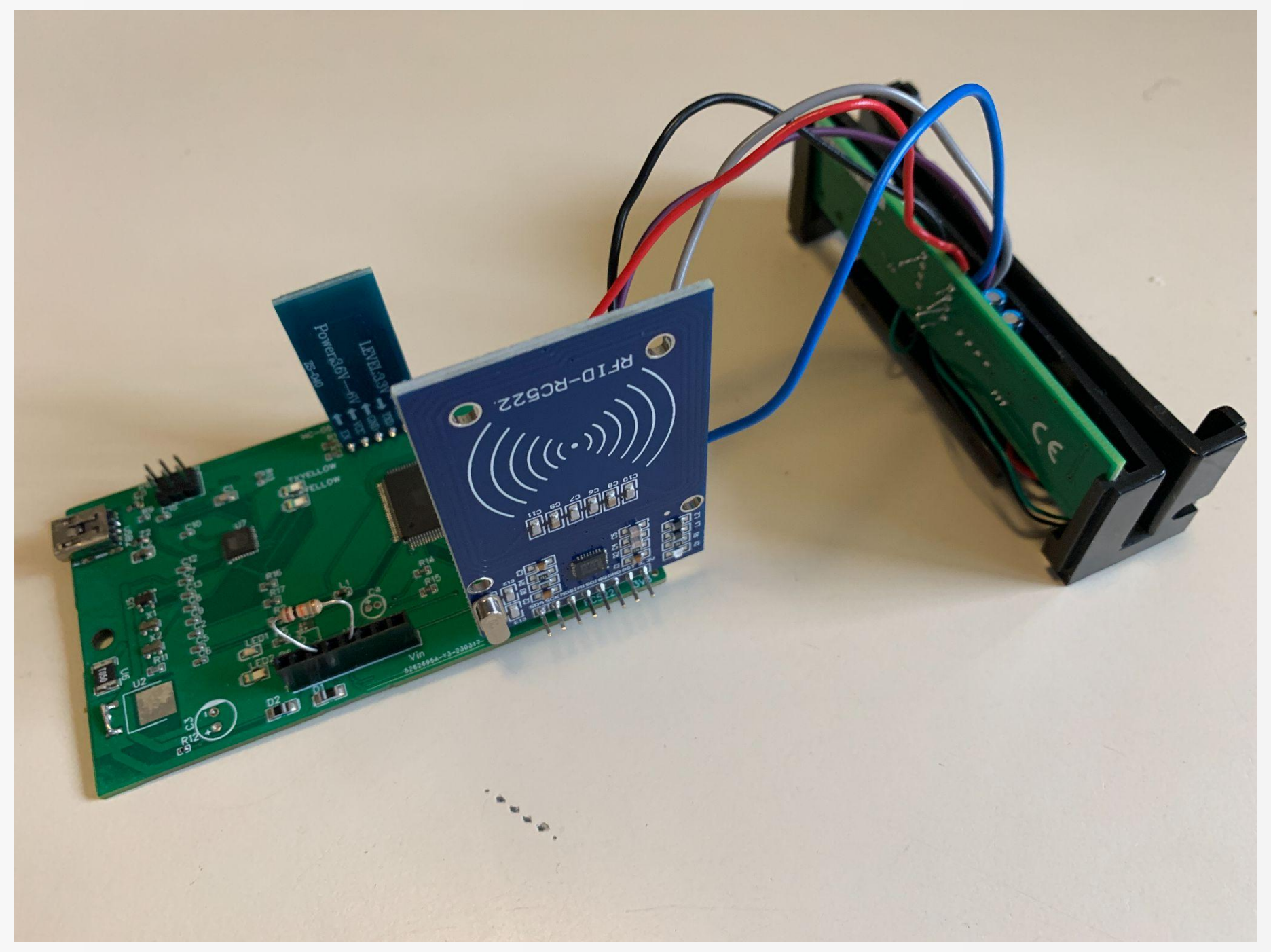
- Software running on the circuit's microcontroller was written using Arduino IDE for ease of use as well as interfacing with the Arduino prototype (same ATMEGA2560 chip powers both Arduino Prototype and final circuit design).
- Used existing user-generated libraries to interface with Bluetooth, RFID, and magnetic stripe modules.
- From a standby mode, the microcontroller can receive input from the user to switch it to the RFID or magnetic stripe reader modes, from there choosing whether to exit back to the standby mode or switch to the store/copy read data mode.


Standby Mode
Computer Input Received: Exit Magnetic Stripe Mode
Computer Input Received: Enter Magnetic Stripe Mode
Computer Input Received: Enter RFID Mode
Computer Input Received: Exit RFID Mode
Magnetic Stripe Read Mode: Awaiting Input
RFID Read Mode: Awaiting Input
Magnetic Stripe Card Detected
RFID HF Tag Detected
Computer Input Received: Enter Copy Mode
Computer Input Received: Leave Copy Mode
Card Data is Read and Stored
Tag Data is Read and Stored
Most Recent Tag Data is Prepared
Desired Tag Data is Flashed to Blank Tag

Arduino Prototype Diagram



Finished Circuit with Designed PCB

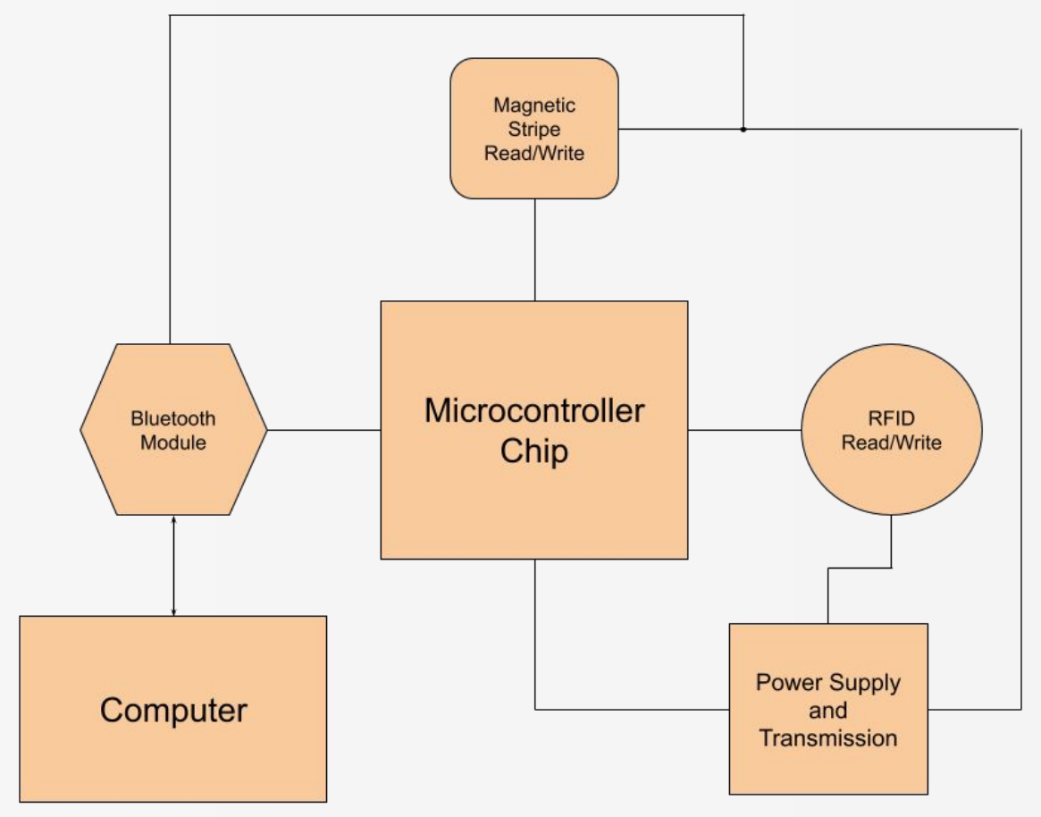


System Design

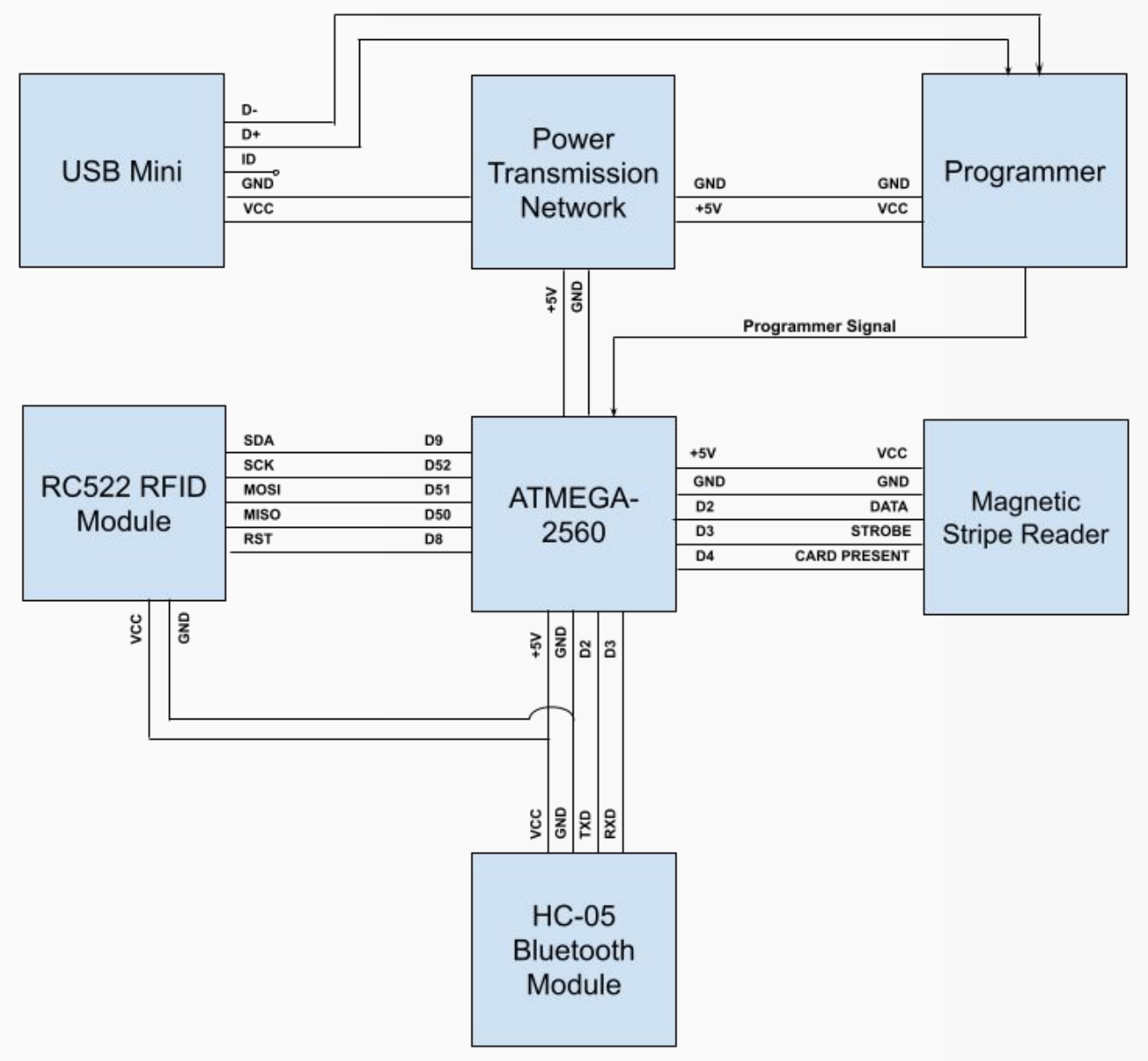
In order to accomplish the task of skimming RFID and magnetic stripe data, the circuit would need:

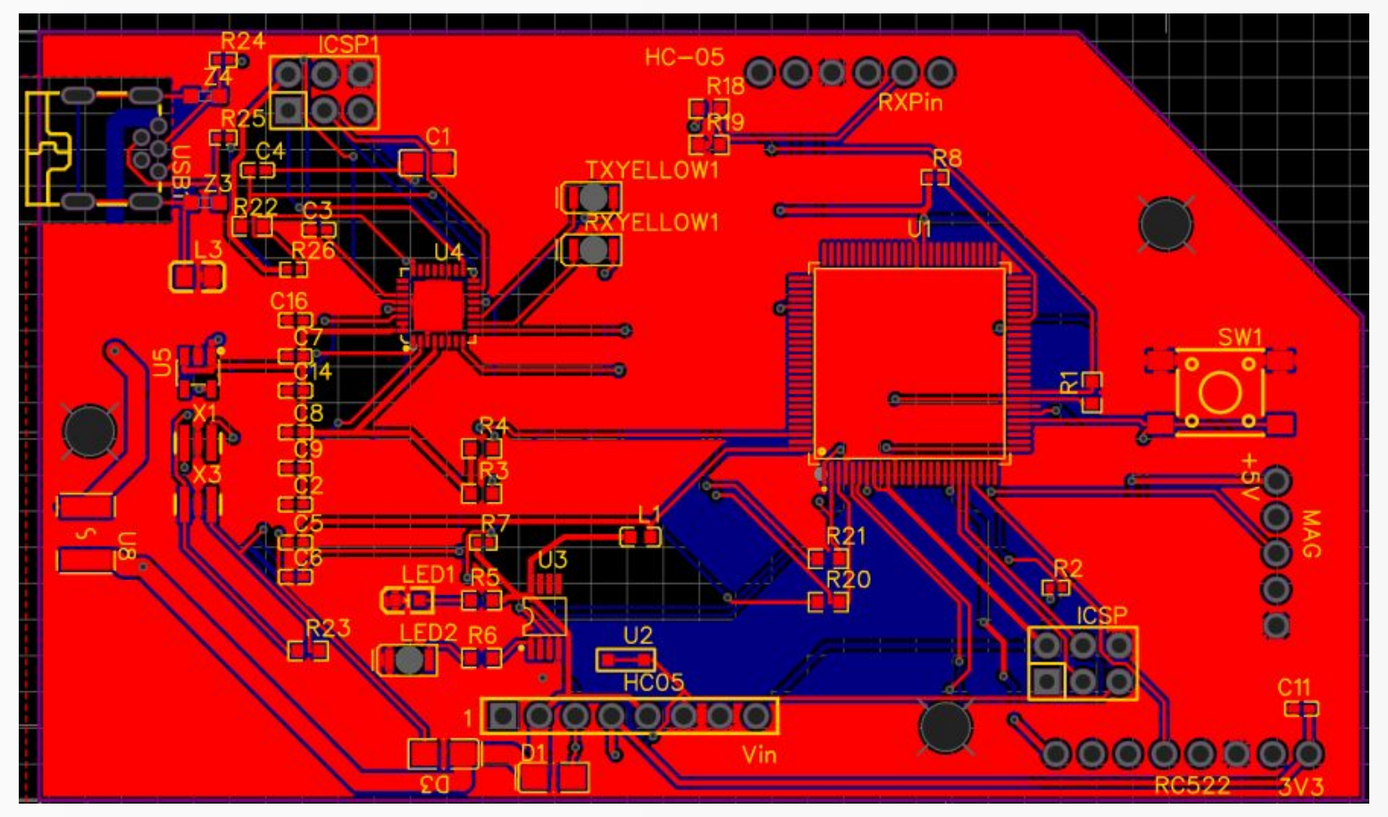
- RFID antenna/reader to read and copy RFID tags
- Magnetic stripe card reader to read and copy magnetic stripe cards
- Bluetooth module to communicate with the main computer
- Power distribution network to power system
- Microcontroller chip to interface with the different modules and collect/analyze skimmed data

The basic configuration for this circuit is shown to the right.



Circuit Design





To keep the circuit simple, an Arduino Mega which was used for prototyping was used as reference for the circuit design. The building blocks of the circuit design were:

- ATMEGA2560 microcontroller chip (ample I/O pins and onboard storage)
- MFRC522 RFID Module which is compatible with RFID HF (13.56MHz) tags (common frequency used for tap to pay and NFC)
- HC-05 Bluetooth module has a small form factor and works well with Arduino or Arduino-based systems
- ATMEGA16U2 microcontroller for interfacing between the ATMEGA2560 and USB (for programming the board)
- Magtek TTL magnetic stripe reader for reading magnetic stripe cards
- USB Mini B for supplying regulated 5V input to the circuit

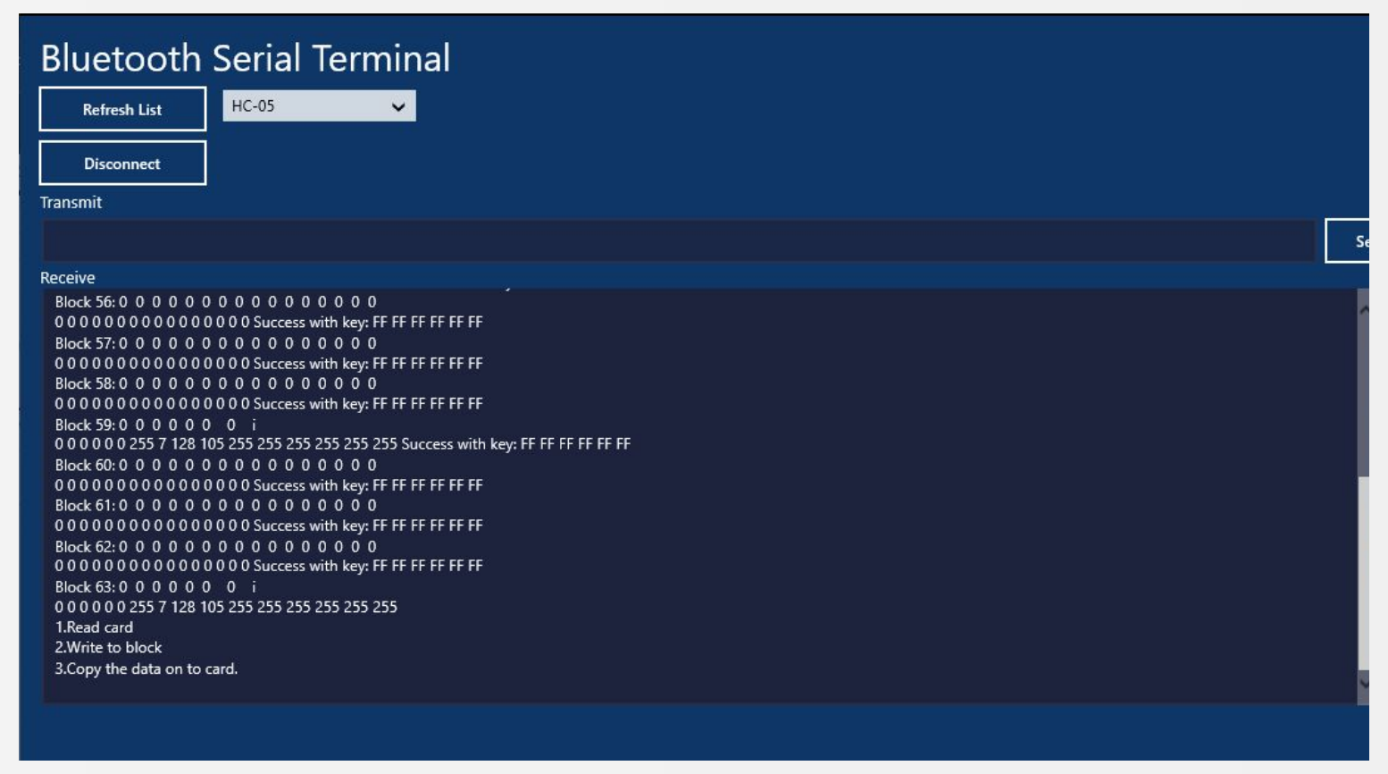
Results

What I learned:

- How to use EDA software to design and test Printed Circuit Boards (PCBs)
- How to implement microcontroller chips in system design
- How to interface microcontrollers with multiple modules and analyze data from these modules

Final Implementation Results:

- Final circuit could read RFID tags and magnetic stripe cards and store their data
- Bluetooth connectivity was achieved for wireless communication between main computer and skimming device
- RFID copying was implemented to duplicate stored tag data onto blank tags
- Magnetic stripe copying was not achieved through the circuit, but card data could be stored and referenced for outside copying



```
Block 56: 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 Success with key: FF FF FF FF FF FF
Block 57: 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 Success with key: FF FF FF FF FF FF
Block 58: 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 Success with key: FF FF FF FF FF FF
Block 59: 0  0  0  0  0  0    0   i
0 0 0 0 0 0 255 7 128 105 255 255 255 255 255 255 Success with key: FF FF FF FF FF FF
Block 60: 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 Success with key: FF FF FF FF FF FF
Block 61: 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 Success with key: FF FF FF FF FF FF
Block 62: 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 Success with key: FF FF FF FF FF FF
Block 63: 0  0  0  0  0  0    0   i
0 0 0 0 0 0 255 7 128 105 255 255 255 255 255 255
1.Read card
2.Write to block
3.Copy the data on to card.
```

Bluetooth Terminal Communication between Skimmer and Main Computer

Conclusions

Most of the design objectives were completed, and the accessibility of this design stands to prove the weaknesses in RFID and magnetic stripe technology.

Future Improvements for Circuit:

- Implement onboard magnetic stripe copying
- Chip reader implementation
- Reduce the size of the PCB (potentially use just one microcontroller)

Security Improvements:

- Phase out magnetic stripe cards completely
- RFID pay is safe for now due to one-time codes generated during transactions

Disclaimer

It should be noted here that the research done in this project is purely for educational and security purposes, all testing done was performed with dummy RFID tags and magnetic stripe cards and no sensitive data was manipulated in the production of this design.