Spade

Chengyun Liu, Romi Phadte, Lawrence Supian

Product Summary

-Payment device
-Vendor-side
-Gets data from cell phone
-Emulates card swipe

Components

iOS

Nordic

Arduino

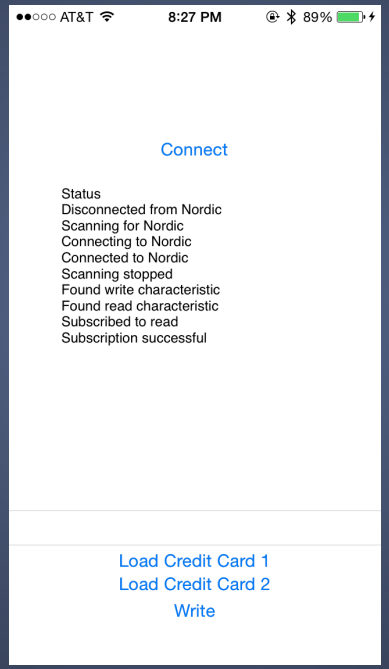
Electromagnet coil

iOS Development

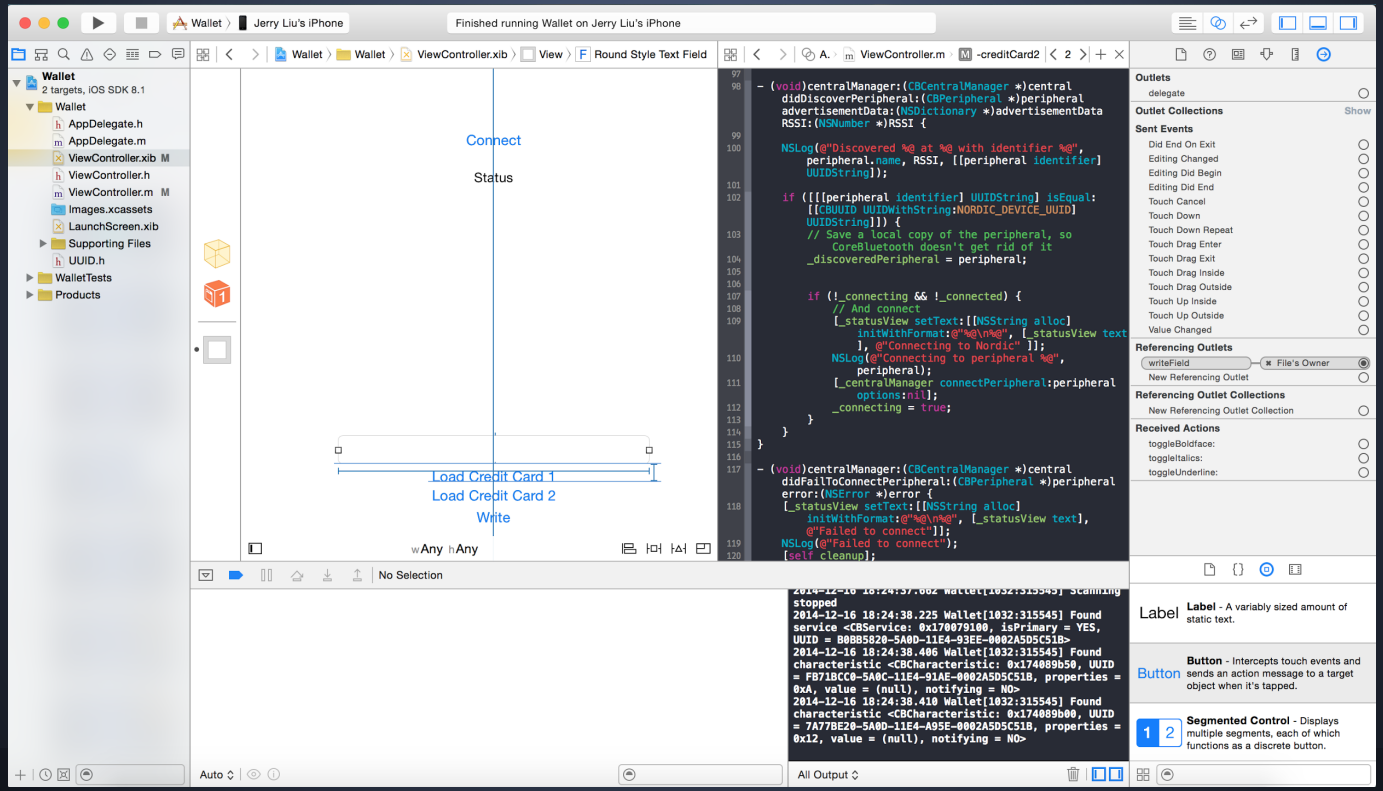
-Language: Objective C
-Tools: CoreBluetooth library

-Function
-App sends credit card data to Nordic board

iOS Development



iOS Development



Nordic Development

-Language: C++

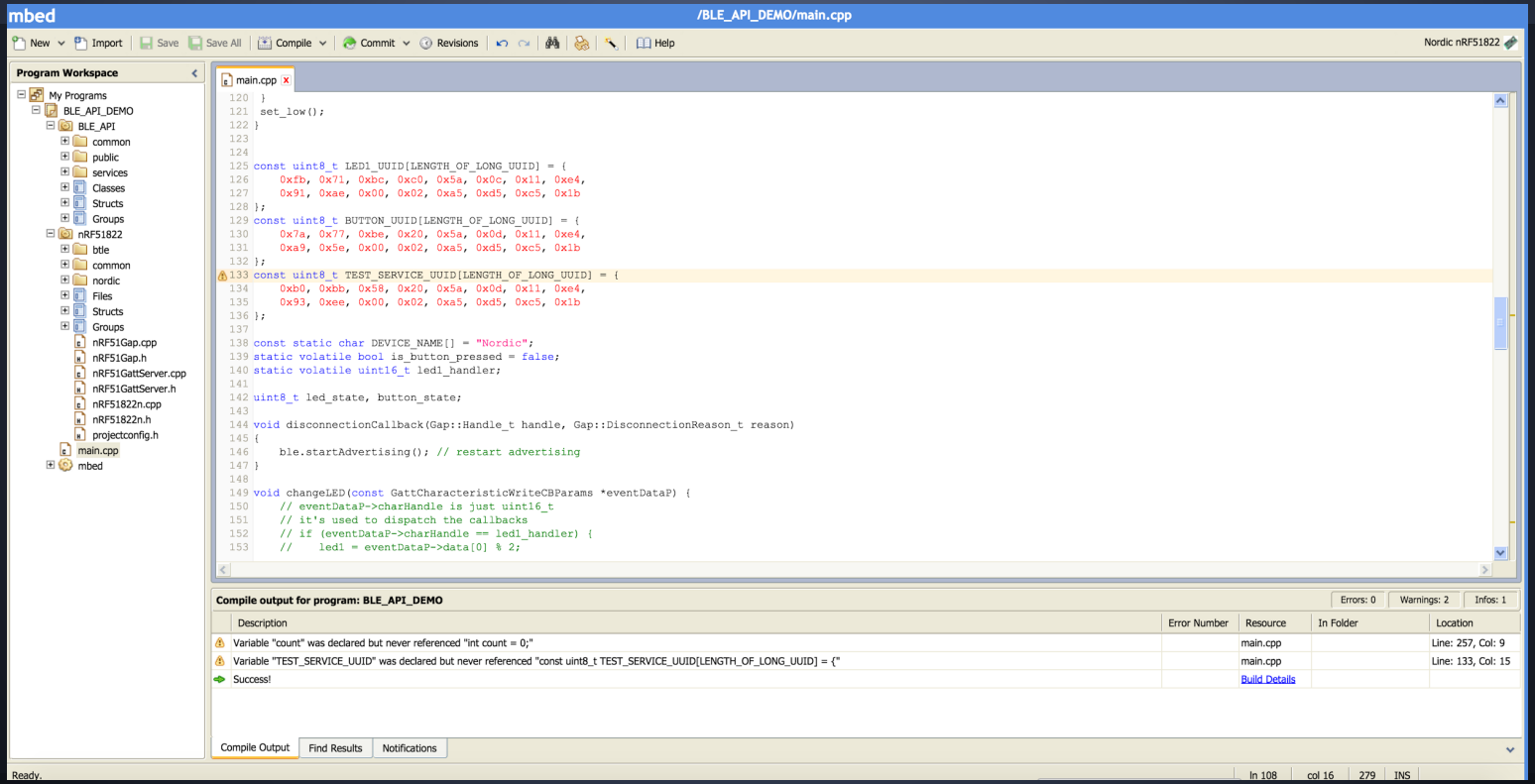
-Tools: mbed platform

-Function?

-Receives credit card data and sends it in binary as digital signal to electromagnet coil at a desired frequency

Nordic Development

Nordic Development



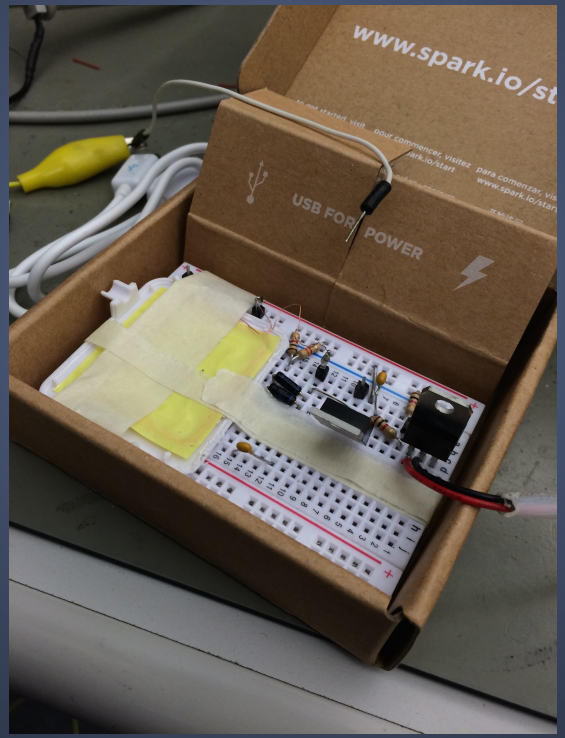
Electromagnet Coil

-Hardware: Multimeter, oscilloscope, Square reader

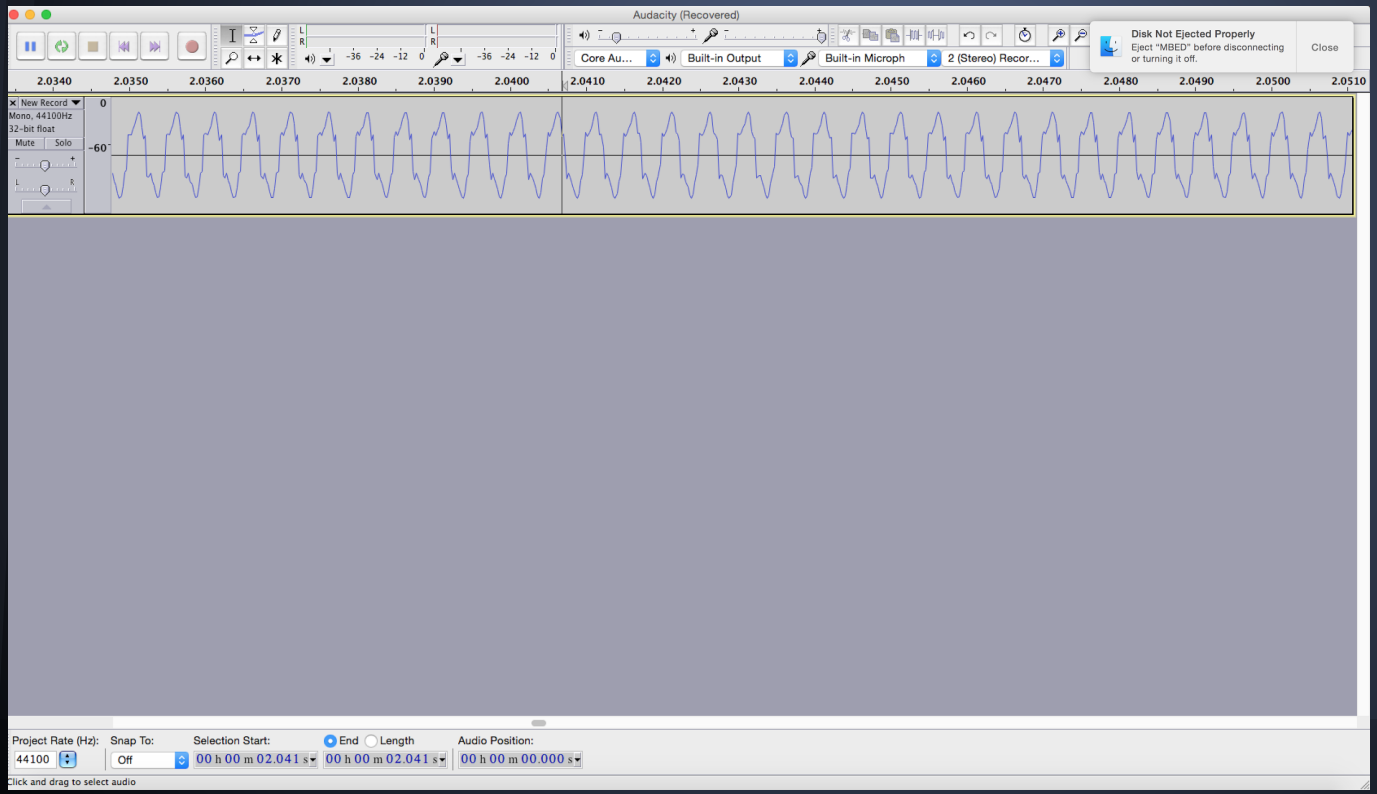
-Software: Audacity, Square app

-Function: Translate digital signal into electromagnetic pulses in emulation of credit card magnetic swipe

Electromagnet Coil



Electromagnet Coil



Theory: BLE

Bluetooth 4.0

-central connects to peripheral, peripherals may have services, services have characteristics, i.e. read, write, notify

-could be useful for communication protocol

-up to 100m range, can detect strength of signal

Embedded Systems: BLE

-communication between devices

-devices in states depending on messages received

-wait and receive next message to “change to next state”

-waiting, sending, acknowledging important because separate, concurrent systems

Testing: BLE

-testing communication

-automatic ack, notification for packets

-large packets failed

-discovered “recommended” limit of 20 data bytes per packet

Theory: Security

Ensure it is the Spade of the vendor we are purchasing from?

-register Spade online with vendor name, public key, location

MITM?

-use nonce

Theory: NFC

Bypass need for hardware with NFC EM?

-not feasible

-13.56 MHz crystal oscillator soldered, not interfaceable

-crystal needed for intended function at NFC 13.56MHz

-thus doesn’t work for us because we need the frequency to be KHz in order to correspond with swipe speed

-source: Texas Instruments NFC Info Sheet http://www.ti.com/lit/sg/slyt493/slyt493.pdf

Testing: Nordic Frequency

-checking Nordic board frequency

-need somewhat better than 1KHz so we can toggle pin at 1KHz

-got >100MHz, definitely more than enough

-delay toggling of pin if necessary to adjust to 1KHz

Theory: Credit Card (Data Level)

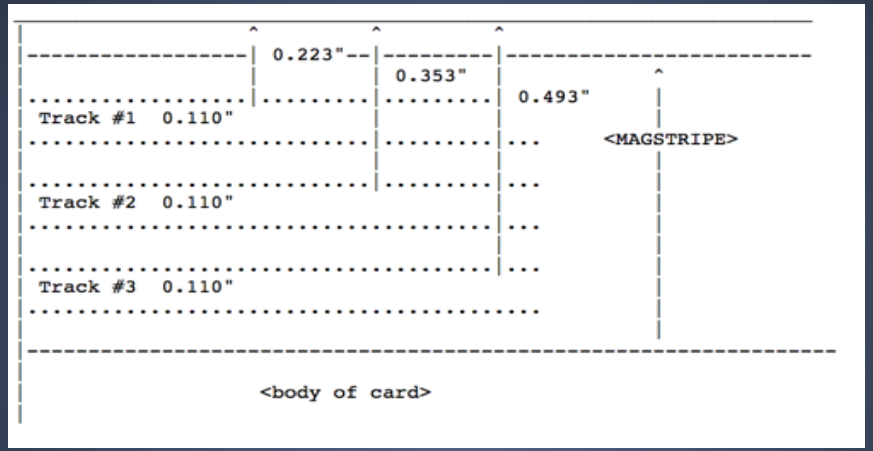
Track1:

%B4465411255386057^PHADTE/ROMI^
1601101100001000000000494000000?;

Track 2:

4465411255386057=16011011000001494?

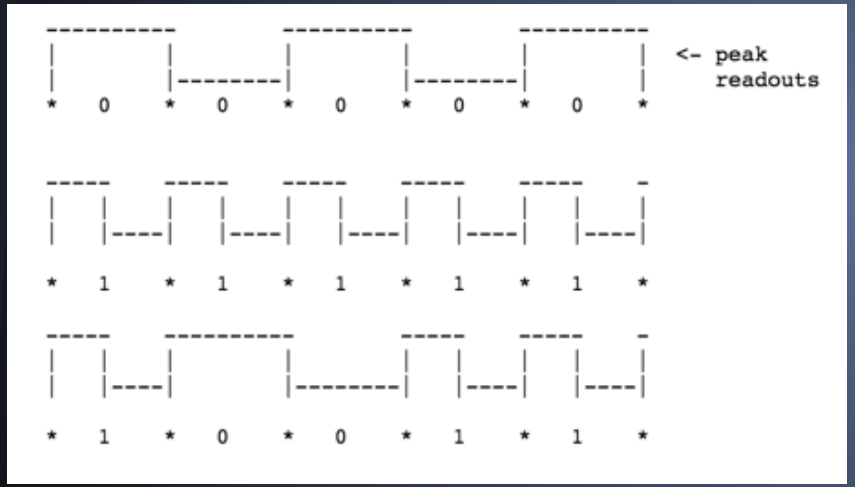
Theory: Credit Card (Protocol Level)



Track	Name	Density	Data-Rate	Format	Characters	Use
1:	IATA	210 bpi	1.05kHz-10.5kHz	ALPHA	79	Name+Account
2:	ABA	75 bpi	375Hz-3.75kHz	BCD	40	Read Account
3:	Thrift	210 bpi	1.05kH-10.5kHz	BCD	107	Encode

Each begins and ends with a sentinel. Humans swipe with speed of 5-50 in/s. We used this to settle on frequencies of about 2-3kHz. This modeling was verified to work in real world tests.

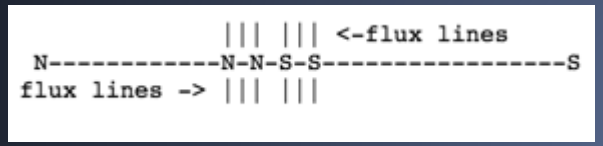
Theory: Credit Card (Byte Level)

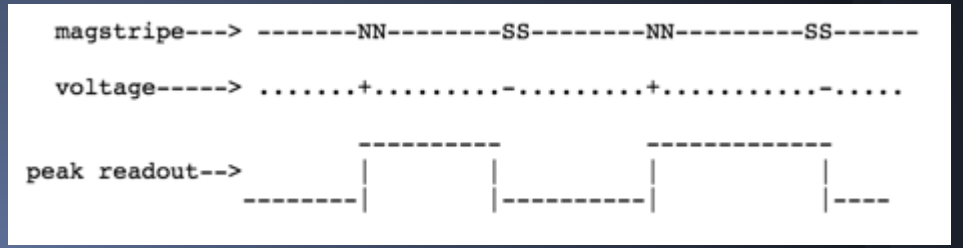


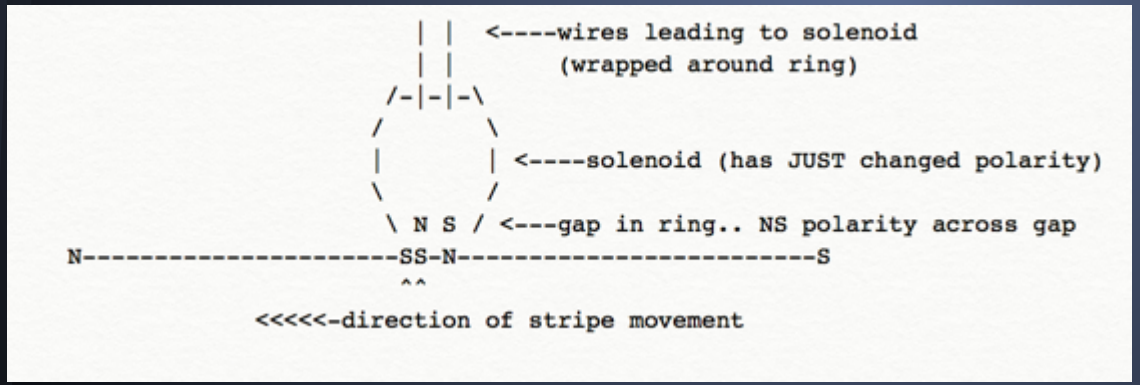
--Data Bits--				Parity		
b1	b2	b3	b4	b5	Character	Function
0	0	0	0	1	0 (0H)	Data
1	0	0	0	0	1 (1H)	"
0	1	0	0	0	2 (2H)	"
1	1	0	0	1	3 (3H)	"
0	0	1	0	0	4 (4H)	"
1	0	1	0	1	5 (5H)	"
0	1	1	0	1	6 (6H)	"
1	1	1	0	0	7 (7H)	"
0	0	0	1	0	8 (8H)	"
1	0	0	1	1	9 (9H)	"
0	1	0	1	1	: (AH)	Control
1	1	0	1	0	; (BH)	Start Sentinel
0	0	1	1	1	< (CH)	Control
1	0	1	1	0	= (DH)	Field Separator
0	1	1	1	0	> (EH)	Control
1	1	1	1	1	? (FH)	End Sentinel

***** 16 Character 5-bit Set *****
10 Numeric Data Characters
3 Framing/Field Characters
3 Control Characters

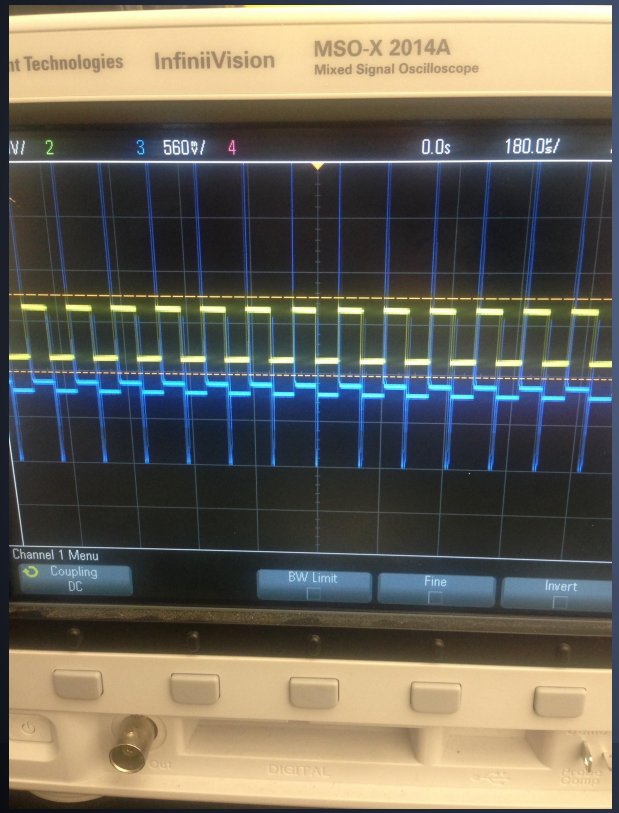
Theory: Credit Card (Physical Level)







Testing: Electromagnet Emulation



$$v(t) = L\frac{di}{dt}$$

$$V = IR.$$

Next Steps

Create custom PCB for circuit.

Miniaturize device.

Improve app

Remove Arduino.