SPADE

Mobile Payment System

Romi Phadte, Jerry Liu, and Lawrence Supian, *UC Berkeley*

***Abstract*— Spade is a mobile payment system that hopes to improve the customer payment process by giving users the ability to pay with smartphones. The space system involves BLE enabled hardware to be attached to the payment register. This device accepts encrypted credit card data through BLE and emulates credit card swipes by emitting a changing electromagnetic pulse that can be detected by a traditional read head.**

I. Introduction

SPADE was inspired from the huge capital costs required to upgrade the country's infrastructure to Apple pay and similar mobile payment technologies. There is little doubt that mobile phones will one day replace bulky wallets like they have in Japan and progressive cities around the world. However, the means of that transition has been debated for many years as several huge players including Google, Apple, and Square struggled to decide how the 21st century consumer should pay for goods. The primary drive for huge investment in this space is information. Gaining access to all the stores that a consumer visits and tracking user behavior is an incredibly valuable resource; especially given the ad driven nature of the largest tech companies of this era. Its safe to say that those are able to gain control of this information will have a huge advantage in supporting the ad driven business models of this era.

With over 1.75 billion people owning a smartphone globally, its not a doubt that we are in a new era of computation. These remarkably capable devices come with many useful chipsets such as Wi-Fi, Bluetooth, and NFC.

We are interested with the Bluetooth and NFC technology since these two do not requires centralized server. These two technologies can start the connection between two devices with just handshake initialization.

Bluetooth has been around for few years, and always kept being improved every year. The latest version known of the Bluetooth is very popular because how the Bluetooth can save energy a lot by going to sleep every time it is not being used. Also, Bluetooth is being very popular because of the range span that is up to one hundred meter.

On the other side, NFC, near field communication, is a kindly new developed communication protocol between two devices that can send anything between these two. However, the cons of using NFC is that the lack of range, in which two devices must be very close to each other, or even touch the other to initiate the connection.

However, these two communication protocols are being widely used by many developer to make application now a day because of the easiness to make call function to either receive or send packets to the other Bluetooth or NFC supported device.

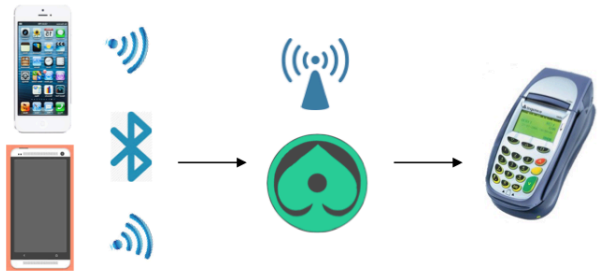
Finally, we also made the electromagnetic generator signal that can emulate the credit card swipe.

II. Spade Payment System

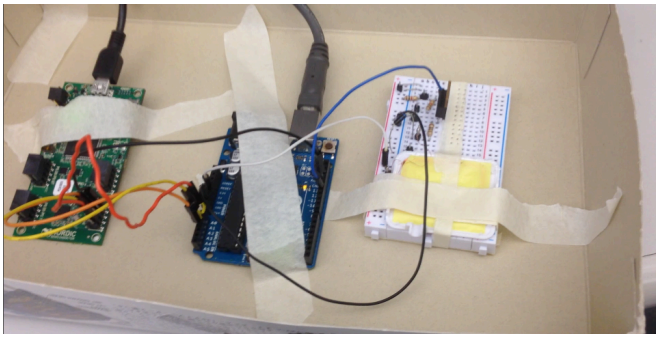
A. Setup

The spade current idea is we want to be able to create an easy plug and play device, so every merchant can just buy this devices and attach those devices easily into the credit card registry without upgrading or buying new hardware and technical expertise to set up the Spade.

We decided that our main prototype is going to look like a black box where there is a black box in the middle of the system that will always advertise the bluetooth signal as the peripheral device. Then, our spade will have sensors input from any of the bluetooth supported device that has our apps. The input will contain data information about the parsed credit card information. And, the actuator will be the electromagnetic signal generator that outputs the signal to the credit card machine for payment. The main layout will look like the following:



Inside our spade's black box, there are going to be only two devices, such as the Nordic NRF51822 equipped with mbed controller and electromagnetic generator. In addition to these two devices, we add an arduino for the prototype purpose because it really helps as the arduino can read the input from the nordic to the electromagnetic generator and print it to the console. The current version of our prototype looks like:



B. Analysis

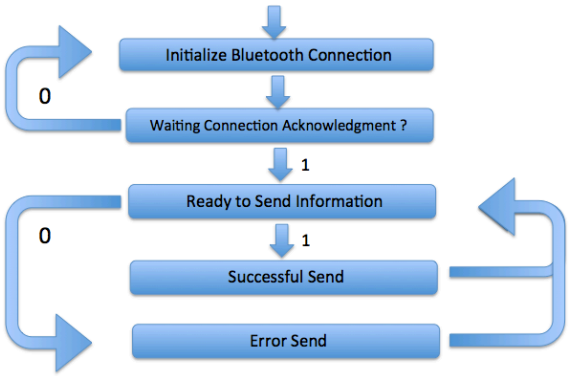
Although, each of the devices in the spade's black box seem very easy to be used or created; in fact, there are a lot of issues that we faced with the devices. We are going to explain the issues and also reasons to choose/ create the devices in this sections including the ios apps to send ble datas to nordic.

B.1. iOS APP

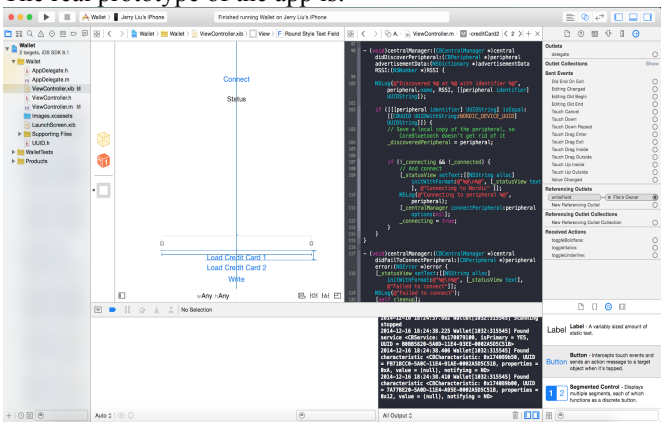
The main function of the ios app is to store the credit card information into the phone's storage, so it can be used later for the payment system. During prototyping time, we hard coded the credit card information from the credit card reader attached to a laptop. However, in the future, we to give input to the app through card reader that is attached to the audio jack to scan the credit card information and stored into the database. For our prototyping, we used a credit card scanner that was attached to the computer and paste that information to the app.

The other functionality of the iOS app that we want to achieve is being able to initialize connection with the Nordic via Bluetooth, read any acknowledgement, and send the necessary informations to the Nordic. At the beginning, this process seems very abstract for us because not only we must find the Bluetooth library from apple, but we don't know how to test it since there is no code has been worked with the Nordic. Luckily, our GSI, Ben Zhang, already made some template application for Nordic that works with the lightblue app that can be downloaded from the apple store. Because of that, our ios app work has some function similarity with the light blue with some tweaks to include more features. We use the corebluetooth library to make the bluetooth connection.

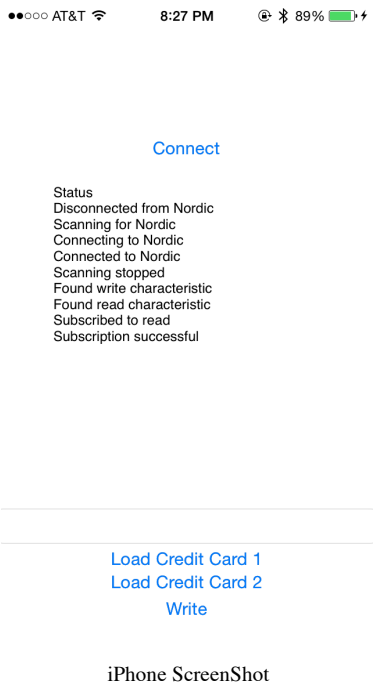
For example, our app can write the stored credit card information into the Nordic with just one press, switch to second credit card information and sent the information, and put custom numbers into the blank field and send it. The workflow of the app is that we start the app with fresh initialization, then search for the bluetooth peripheral, wait for acknowledgment about connection initialization, send information, wait for acknowledgment whether write successful or not, and finally wait for another input. During the prototyping time, we decided to just hard code the nordic's uuid since we only have one device and always constant never change instead of searching for the uuid. The workflow of the app is the following:



The real prototype of the app is:



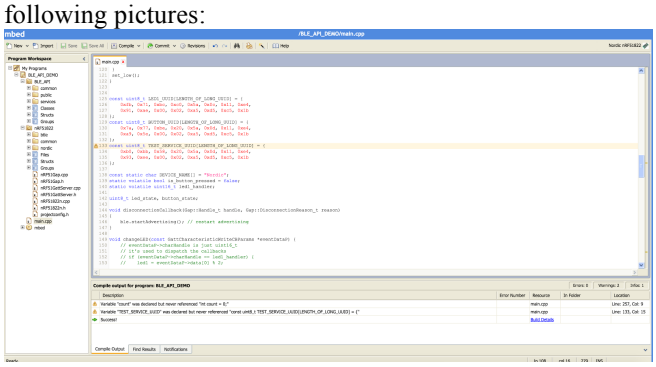
The Xcode Development Screen



iPhone ScreenShot

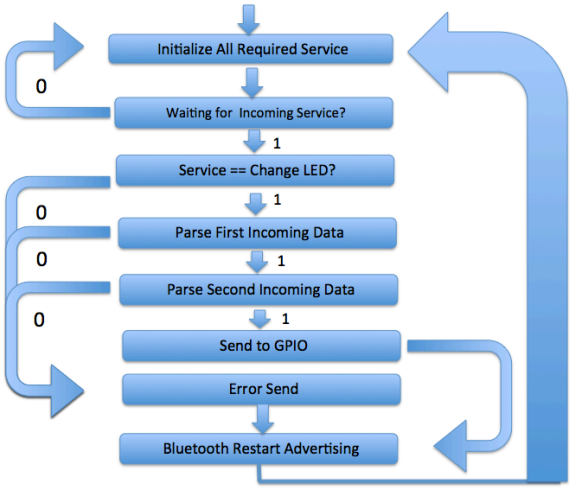
B.2. Nordic NRF51822

Nordic NRF51822 is one of the useful microcontroller in the factory because it is supported by the mbed that has bootloader supported. It is very useful to be supported by the mbed because it is very easy to bootload a code that we wrote. It is just in matter of seconds to compile and push the code into the Nordic board via mbed without installing anything new in any operating system. For example, like the following pictures:



Other than mbed, nordic is very powerful because of its support for the BLE, Bluetooth low energy. It is good in our purpose because we can use watch battery to power up the nordic for very long time. Considering, the BLE is an advanced scheduling for Bluetooth in which the device will go to sleep or idle when there is no incoming connection, but once there is an incoming connection it wakes up. So we can leave this device for months with battery power at the registry machine.

The code for this nordic has been developed before by our GSI, Ben Zhang; and we add some more lines of code to make the device parse the credit card information, such as the parity information; and also set the correct frequency for the signal. The Nordic's state diagram is the following:



One of the great benefits that nordic has is that the frequency of the GPIO is sixteen megahertz. That is more than we expect, but it is good enough because in order for the swipe to be working the frequency should be at least one kilohertz.

We did many trial and error to come up with this number by using the wait function inside the mbed code to slow down the frequency. The pin that we use is basically the led pin because it comes with the template and the led pin has GPIO as well.

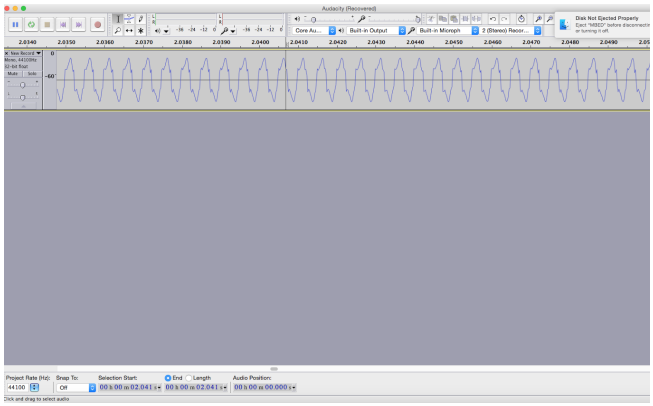
Finally, in order to help our prototyping, we use arduino in the middle of the nordic and electromagnetic generator. The arduino really helps us because it can print exactly what binary data being passed into the electromagnetic generator since we calculate the value inside our nordic and passed it out through gpio.

B.3 ElectroMagnetic Generator

The last component of the device is the electromagnetic generator. Credit cards produce an electromagnetic signal an a read head when it is swiped through a credit card machine can read it. Because of that, we create a system that can produce the generate electromagnet that can be detected the credit card machine.

This last part is kindly the major difficulty because there is not many people already design/ sell it and put it on the online as the open source. Because of that we must design our system to clean the signal, but strong enough to be caught by the credit card generator.

In the first of our trial, we started by catching whatever noise is being generated by using microphone. The resulting output is the following:



Once, we got the good looking signal, we tried to make it work with the nordic and the ios app. At the beginning, it did not work because there are miscalculated resistor and transistor that cause the signal too low and can't be detected by the card reader. We debug it using the oscilloscope and waveform generator to see how each of the part on the board working. Luckily, it is working at the end after few days debugging. In order to test our result, we use the square reader card because it represents the real credit card reader and can be easily bought out there. This square card reader will be attached to an iPhone that has Internet connection to check whether the card is good to be used or the fraud one. The square card reader we have looks like below:

B.4. Considerations and Future Work

1. NFC - near field communication

We are thinking about making the spade using the nfc technology to connect directly from the phone to credit card registry since it become more and more popular now a day because of the easiness to use it. However, we tried to find some resources about this, but it doesn't work because the frequency that it has is too high for a swipe of credit card. In fact, they have 13.56 MHz crystal oscillator soldered and not ineffaceable at all. Because of this, the frequency is too high, and there is no way to make the frequency go lower because the crystal will not work properly any more if the frequency is stepped down. The resources we get is from: http://www.ti.com/lit/sg/slyt493/slyt493.pdf

2. Security

We are thinking to improve our security by using the gps location to defeat theft and replication, nonce for transactions that will counter attack the MITM, and added with user's specific information encrypted with the unique public key to prevent spoofing. Because of that, we require each vendor to register to us, so they can register the public key that the spade's has with our database.

III. Conclusion

We came up with the idea of the spade, which is very broad range because there are many ways to implement the spade. However, Bluetooth communication protocol is one of good idea because it serves the easiness to establish connection between each device. Also, the state machine diagram is very useful in our design because it gives every thing very clear idea and easy to follow. And also the simulation strategies is very important in testing our product