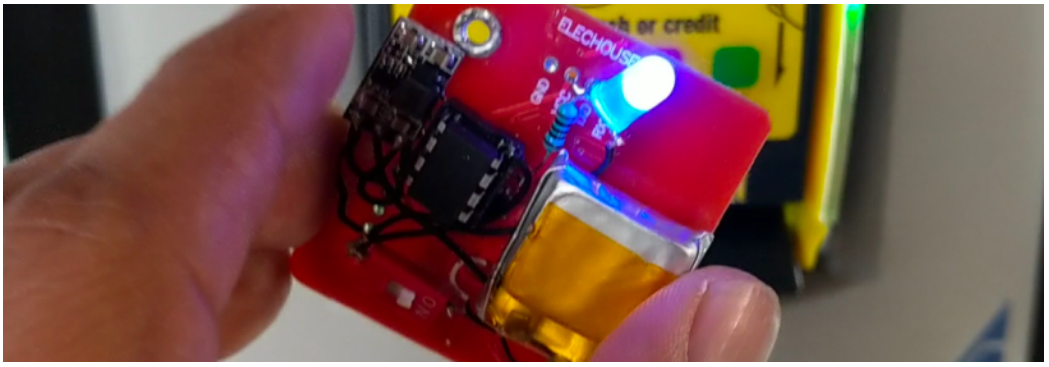
Salvador Mendoza

If you are not making something or inspiring something, you are doing something… wrong.

TOOLS

NFCopy85



Date: June 16, 2019Author: Salvador Mendoza 0 Comments
NFCopy85 is a 10 dollars device to make replay attacks against NFC payment systems. Tested it against Samsung Pay, Google Pay and Wells Fargo Wallet NFC tokens in US.

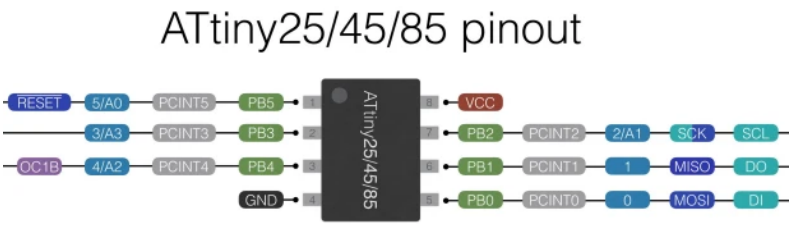
Hardware

NFCopy85 is a small version of NFCopy. This tiny version is a combination of ATtiny85 and a small PN532 board. Adding a 3.7 LiPo battery and a power booster to increase the 3.7V to 5V for the PN532 board. Also I added a LED with a resistor just for debugging and to show activity.

Software

For the software side, I modified the Adafruit PN532 library. By default, the library is too big for the ATtiny85 and some functions had to be edited for a good communication between the ATtiny85 and PN532 board. To establish the communication, I decided to use SPI. So I deleted all the parts in the library that were not needed for the SPI communication.

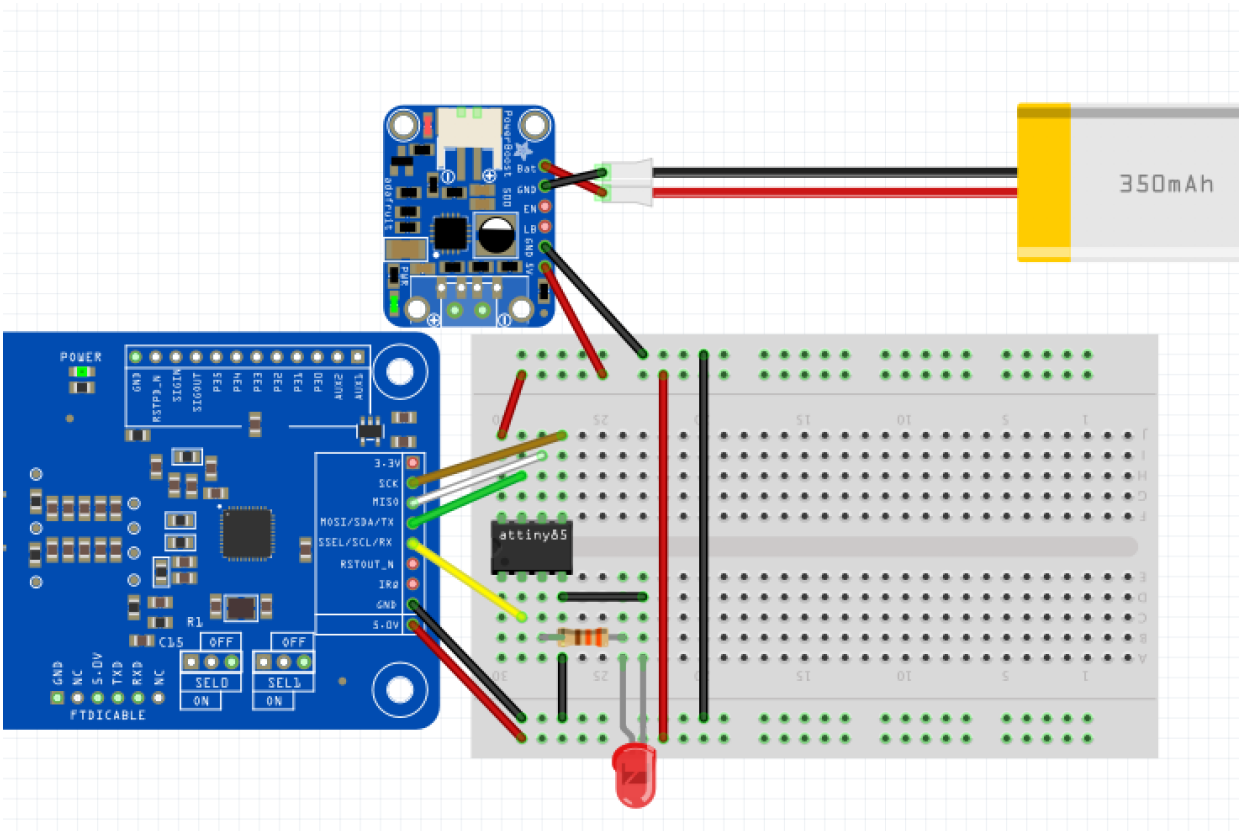
Wiring



In order to connect the ATtiny85 and the PN532 board, I used the SPI connector from the PN532 and the USI (Universal Serial Interface) from the ATtiny85.

In my PoC, I used the pins 0, 1, 2, 3 for PN532 SPI and also the 3 for the LED. But in the code I assigned 4 for LED. Why? I was using the pin 4 for debugging(which was a nightmare)

```
define PN532_SCK  (0)
define PN532_MOSI (2)
define PN532_SS   (3)
define PN532_MISO (1)
define LED   (4)
```



PoC

I designed a small program to make a replay attack using the Visa MSD protocol. In this case, I used a Google Pay token which was previously intercepted.

Code

PoC: https://github.com/salmg/NFCopy85/blob/master/NFCopy85.pde

Library tinyPN532.h: https://github.com/salmg/NFCopy85/blob/master/tinyPN532.h

Note: This PoC was recorded using the US payment system. If you noticed that the NFCopy85 code does not check or use the terminal's response because it assumes the commands, but this could be different in another country or in another payment system.

If you want to be the first to know about my projects, support my research at https://www.patreon.com/salmg

ADAFRUIT ATTACK ATTINY85 AVR NFC NFCOPY NFCOPY85 PAYMENTS PN532 REPLAY RFID

Published by Salvador Mendoza

View all posts by Salvador Mendoza