# Designing an Inconspicuous RFID Sniffer

Nathan Tarrh

nathan.tarrh@tufts.edu

Ming Chow

**Abstract**

Radio-frequency identification (RFID) is a growing attack vector in systems around the globe. As ease and cost have made RFID more popular for identification, inventory tracking, and payment systems, methods for cracking RFID systems have become equally cheap and straightforward to implement. I present a design for a simple, portable cracker that can readily sniff low-frequency, passive RFID chips.

# 1 Introduction

Even if you've never heard of RFID, you're surrounded by systems that use it. Any time you take a plastic card and tap it against a panel instead of swiping, you're actually creating a magnetic field that resonates between the card and the panel, allowing your card to send an identifying code to that panel (Norman, 2012). The problem here is that anyone who can create a similar resonant field near your card can copy your access code!

Brown (2013), and Meriac (2010) among others have described systems for analyzing the information stored on chips that transmit data using the RFID protocol, but focus less on systems for obtaining that data. Brown, in particular, presents a long-range RFID stealer that can obtain data from up to 3 feet away. What he doesn't focus on is that his solution is nearly 12 inches by 12 inches square—hardly inconspicuous on public transportation or in a coffee shop.

I present a discreet, portable RFID sniffer that leverages open-source hardware prototyping tools. Given that I have very little background in hardware projects, this tool will show how simple it is to create a sniffer using commercially-available products. Once the device has been established, I will also discuss a small amount of material related to attack prevention.

## 2 To The Community

Take a look at your purse or wallet. Do you use a card that you tap against a turnstyle for access to public transportation? Do you have a student ID that lets you into a dorm? Does your workplace have identification cards that give you access to the building, even when no-one is around? Does your coffee shop of choice hand out mobile payment cards that you can tap at the register instead of swiping?

Chances are, you have at least one RFID-enabled piece of plastic on your person, maybe more. How many contain personal information? How many can be used as payment? By showing how easily an RFID sniffer can be built, I hope to demonstrate just how insecure it is to depend on such systems for unique identification, and encourage you to take steps to protect your information from RFID-sniffing attacks.

# 3 Applications

Here at Tufts University, there are two RFID-enabled systems that almost every person on campus uses: Tufts IDs and CharlieCards. CharlieCards use a known authentication protocol, MIFARE Classic, with several studied cryptographic weaknesses (Ryan et al., 2008). As of 2007, the MIFARE encryption has been completely cracked by researchers at Radboud University (Koning Gans et al., 2008).

If you look on the back of a Tufts ID card, you will see in small print on the bottom of the card, "HID iCLASS GH", indicating that the card uses the iCLASS$^{TM}$protocol. A recent paper by Milosch Meriac at the Chaos Communication Congress presented an analysis of the iCLASS$^{TM}$Standard Security encryption and extracted the secret keys, although they were not shared (Meriac, 2010).

Essentially, the encryptions for the systems backing both CharlieCards and Tufts IDs have been compromised, meaning that even if the MBTA or Tufts University were to leverage some form of cryptography, once you have obtained a user's RFID information, that code can be unlocked and spoofed. I designed and developed a portable device that will log RFID information that can later be written to a new RFID card.

## 3.1 Project Design

To build the initial version of the sniffer, I chose to take advantage of the ease and availability of open-source hardware prototyping platforms; namely, the Arduino ecosystem. Because of the recent popularity of Arduino projects, there are several extensions, or "shields", that make a project of this scope trivial to undertake. Additionally, the small size and low cost of the Arduino board played a role in choosing it over, say, a Raspberry Pi, for a portable and discreet project.

### 3.1.1 Hardware

I chose to use three specific pieces of hardware for this project: the Arduino Uno, a microcontroller board based on the ATmega328 chip; the Parallax RFID Reader Module, for reading RFID signals; and the SparkFun microSD shield, for logging data. The Arduino is an electronics prototyping platform. It's designed to be flexible and easy-to-use by providing 14 digital I/O pins that are programmed with a microcontroller to react on the information they receive. The Parallax module is a low-cost RFID reader that requires 5 volts of power and communicates through a 2400 baud Serial interface—the Arduino will provide power to the unit as well as manage the communication. Finally, although the Arduino does have 32k of onboard memory, the SparkFun microSD shield is for easier, more efficient data-logging: we can load code once onto the microcontroller, log data to the shield, and then only deal with unplugging and reading a microSD card rather than read byte-by-byte off of

the Arduino to recover information.

In addition, I experimented with a variety of enclosures to find a suitably inconspicuous fit. I had hoped the project would be small enough to fit inside a cigarette carton (which the Arduino does on its own) but the Parallax shield is too wide for a standard carton. A Gameboy case is covert and would be feasible, because the RFID signal can transmit through plastic (Frenzel, 2005), but I did not want to waste a Gameboy on this project (although a malicious sniffer might). Eventually, I found a Band-Aid carton not much larger than a standard cigarette carton that was able to fit both the Arduino and the reading module and be sufficiently covert.

### 3.1.2 Software

The software behind the Arduino-based logger is extremely straightforward. When developing code for Arduino systems, the board uses two functions: `setup()`, which is run once when the board powers on, and `loop()`, which is run continuously after `setup()` is called.

The setup function (fig. 1) deals primarily with activating the board's digital I/O pins. `Serial.begin()` initializes the Arduino's Serial I/O to the same baud rate as the Parallax board for correct communication. The `pinMode()` functions simply set certain pins to interact with the attached shields. Finally, `card.init()`, `volume.init()`, and `root.openRoot` initialize and mount a filesystem on the microSD card for reading and writing.

The loop function (fig. 2) handles the actual process of using the Par-

Figure 1: The `setup` function

```
void setup() {
  Serial.begin(2400);
  pinMode(RFID_ENABLE,OUTPUT);
  pinMode(CS_PIN,OUTPUT);
  card.init();
  volume.init(card);
  root.openRoot(volume);
}
```

Figure 2: The `loop` function

```
void loop() {
    enableRFID();
    getRFIDTag();
    if(validCode()) {
        disableRFID();
        writeCode();
        delay(2000);
    } else {
        disableRFID();
    }
    Serial.flush();
    clearCode();
}
```

allax board for reading and writing. `enable` and `disableRFID()` determine whether the board prepares itself for Serial input, `getRFIDTag()` reads from Serial-in byte-by-byte and stores it in a buffer, `validCode()` ensures we write a full RFID identifier, and `writeCode()` handles writing the buffer to the mounded filesystem.

The full code for this project, with some documentation, exists online at `http://github.com/natetarrh/rfid/`.

# 4 Summary

With low-cost, open-source hardware and tools I was able to build a low-power, discreet RFID sniffer. It can be powered by USB port, wall outlet, or battery pack, and carried in small enclosures no bigger than a standard

cigarette carton. However, when attempting to log Tufts ID and CharlieCard data, multiple issues arose. In the following section, I will discuss those problems as well as the ramifications in general for continuing, wide-spread adoption of RFID technology.

## 4.1 Results

With the supplied implementation, my sniffer will log data from low-frequency passive RFID chips. It's important to note that there are multiple frequency levels in the RFID standard: low-frequency (LF), at 125kHz; high-frequency (HF), at 13.56MHz; and Ultra-High-Frequency (UHF), between 860-960MHz. The Parallax module I use will only resonate at 125kHz, and will therefore only be suitable for sniffing data from the lowest-frequency cards.

As it happens, both the iCLASS$^{TM}$cards that Tufts uses and the MIFARE CharlieCards both operate at 13.56MHz, the higher frequency. Since higher-frequency reading modules are typically more expensive, I did not purchase another shield to test, but the theory behind my sniffer applies equally to the frequency levels with regards to ease of sniffing. In fact, it's even easier, because the higher the frequency of a card, the longer the possible distance necessary to activate it (Brown, 2013). However, because the electronics prototyping kits deal with data at such a raw, low level, it's very likely that much of my code would need to be reworked to integrate a high-frequency reader. Both the I/O pins, as well as the baud communication rate, would be altered, but the fundamental security issues with using RFID as a unique

identification system remain the same.

## 4.2 Discussion

With the prevalence of RFID systems in use today, it should be harder to implement sniffing and spoofing mechanisms. Yet with practically no experience in hardware prototyping, I was able to construct a viable sniffer that can be carried around on a day-to-day basis to log identification information. I used a few store-bought hardware kits to make my life easier, but the basic resonating circuit can be built simply by winding copper wire and coding a microcontroller with some sort of programmer, all very cheaply. The bottom line is that even if progressing from magnetic swiping to electromagnetic fields is making our lives easier, it's also making them less secure.

Five years ago, a group of students in a security class at MIT sought to examine the weakness of the MBTA system(Ryan et al., 2008). As part of their project, they explored weaknesses in both the CharlieCard and MagCard payment systems. Not only were they successful in completely reverse-engineering the MagCard encryption, they were able to sniff MBTA turnstiles to repeatedly add $5 fares to CharlieCards. After a potential lawsuit, those students are now working with the MBTA to fix the vulnerabilities. Using RFID as a payment platform is seriously insecure, and it's still a problem today.

Even more recently, the Tufts Medical Center implemented an inventory-tracking system that depends on 13.56MHz high-frequency RFID technol-

ogy(Roberti, 2012). While the new, sophisticated system has saved the school money, it's introduced a potential weakness disguised as security. The system works by tagging items with unique identifiers, and placing them in a cabinet that has a built-in RFID interrogator, so that whenever an item is removed it goes out of range and the inventory is decremented. A malicious user seeking to embezzle medication from the system—every single product is worth more than $50 (Roberti, 2012)—needs to simply clone the RFID badge, write it to a new device—which are worth cents, not dollars—and replace the expensive item with the new badge. Using RFID as an inventory platform, then, is also a serious current-day problem.

Additionally, RFID systems can be used to track users, a serious breach of privacy. Programs like the "smart" student ID cards in the San Antonio school system (URL `http://www.nisd.net/studentlocator/`) are being implemented to track the location of pupils throughout the school day. And with public fare payment systems like the CharlieCard, the card-bearer's movements can be mapped simply by following the turnstyles the card-bearer pays at. Finally, toll-payment systems like E-ZPass also leverage RFID technology, and so transmission antennae on and off the highway can be used to track the movements of cars that contain E-ZPass devices. And, because of the insecurity of the RFID mechanism, all these actions can be spoofed by a malicious user seeking to incriminate a third party.

On the *RFID Journal* website, there is an FAQ discussing the potential benefits and downsides of RFID technology. As of December 2013, they don't

hesitate to address potential health hazards and possible layoffs, but not one question out of the 30 addresses the issue of security (RFID Journal). Why is this? I argue that it arises out of a fundamental misconception about how RFID is supposed to be used.

Ultimately, industries are looking at RFID like a fingerprint, when they should be seeing it as a barcode. The ease with which RFID codes can be sniffed and spoofed makes radio-based technology untenable for personal identification and payment systems, and this project demonstrates just how easy it is to develop a basic RFID sniffer with a minimum of tools and experience. This begs the question: how can we protect ourselves?

At a systematic level, we need to stop placing our trust in basic RFID mechanisms. Recent developments in two-factor authentication for websites could integrate well with current RFID technology. At the individual level, there are RFID shields for cards that can be used to prevent close-range sniffing attacks, and employees need to be more careful about where they wear their badges in public (Brown, 2013). At the end of the day, we simply need to rid ourselves of the false sense of security RFID-based systems have given us.

# References

Brown, Francis. RFID Hacking: Live Free or RFID Hard. *Black Hat USA*, August 2013.

Frenzel, Louis E. Open communication: Radio frequency identification. *Nuts and Volts*, June 2005.

Koning Gans, Gerhard; Hoepman, Jaap-Henk, and Garcia, Flavio D. A practical attack on the mifare classic. In *Proceedings of the 8th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications*, CARDIS '08, pages 267–282, Berlin, Heidelberg, 2008. Springer-Verlag.

Meriac, Milosch. Heart of Darkness — Exploring the Uncharted Backwaters of HID iCLASS Security. [27th Chaos Communication Congress presentation; online; accessed 7-December-2013], 2010. URL `http://www.openpcd.org/images/HID-iCLASS-security.pdf`.

Norman, T.L. *Electronic Access Control*. Butterworth-Heinemann, 2012.

RFID Journal. Frequently Asked Questions. [Online; accessed 7-December-2013], 2013. URL `http://www.rfidjournal.com/site/faqs`.

Roberti, Mark. Tufts Medical Center Saved $1.5 Million with RFID. *RFID Journal*, September 2012.

Ryan, Russell; Anderson, Zack, and Chiesa, Alessandro. Anatomy of a Subway Hack. [DEF CON presentation; online; accessed 5-December-2013], 2008. URL `http://web.mit.edu/zacka/www/subway/`.