# Magstripe Hacking

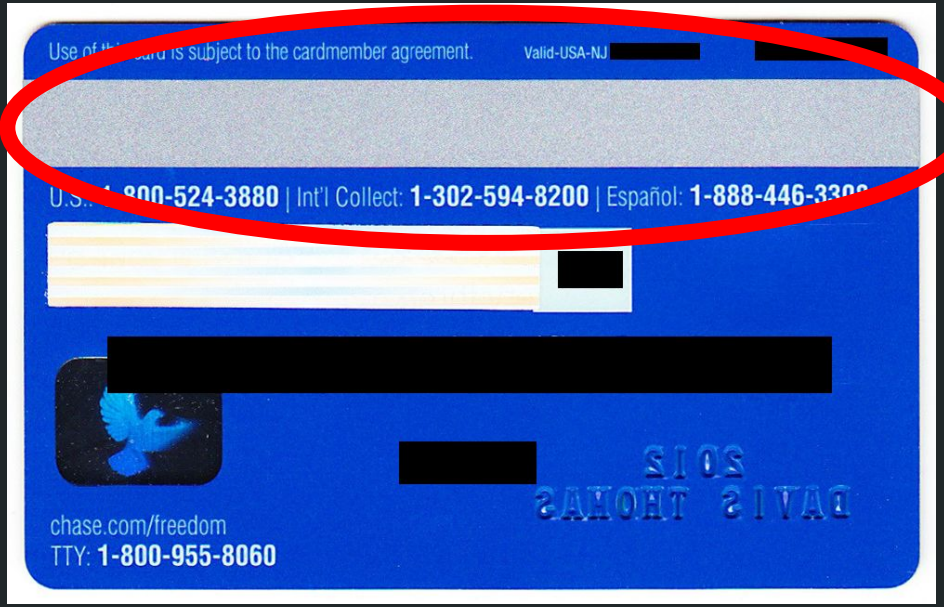
Magspoof, Credit Card Fraud, and other ways to hack a Magstripe

# Presentation Overview

- What is a Magstripe?
- Magspoof
- What can be attacked?
- Copy a UNCC ID

# What is a Magstripe?

A card with a magstripe is capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card. The data is read by swiping the card past a magnetic reading head.



# Magstripe Uses

Some common uses of magstripe cards are...

- Credit/Debit Cards
- Identification Cards (Our Student IDs have a magstripe)
- Security Access Cards
- Parking Garage Cards
- Hotel Keys
- Metro Cards
- Gift Cards
- Etc...

# Why should I care?

- Magstripe cards have such wide usage they make a wide variety of potential targets.
- Everything from Credit Card fraud to unauthorized building access can be achieved by manipulating a magstripe.
- You might also get free parking

- Later in the presentation I will even show how easy it is to clone someone else's UNCC ID Card

# Disclaimer

- Manipulating a Magstripe for personal use is fine, but...

Using a magstripe to steal, gain unauthorized access, commit fraud, and any other crimes will land you in jail.

Don’t do anything that would land you in jail.

I won’t visit you.

# How is data stored on a Magstripe?

# Magstripe Data Example

When scanned here is how a credit/debit card looks...

Track 1
%B0123456789012345^LASTNAME/FIRST^YYMMSSSDDDDDDDDDDDDDDDDDDDDDDD?

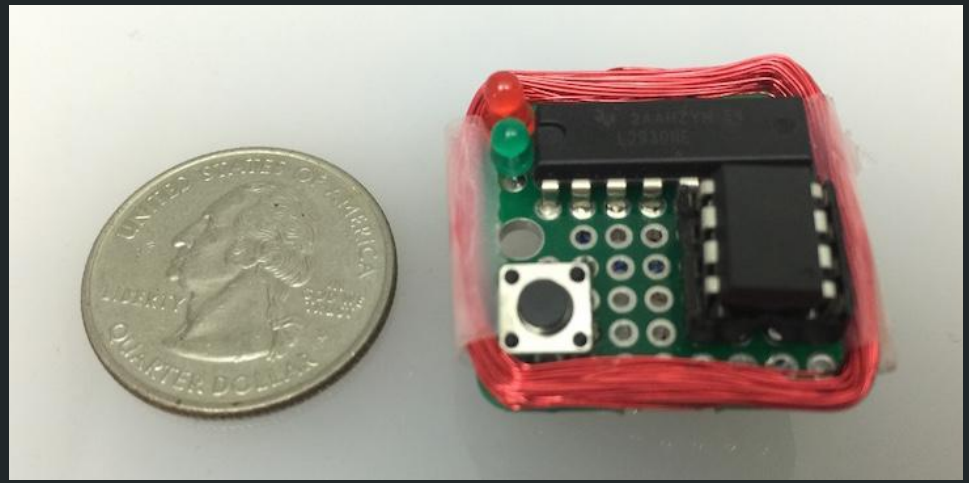
Track 2
;0123456789012345=YYMMSSSDDDDDDDDDDDDD?

Track 3
No Data

# How to Manipulate Magstripe data

MSR605 Reader/Writer


Magspoof



## MSR605 Reader/Writer

- Read any card
- Write to blank cards or modify existing cards
- Supports tracks 1, 2, & 3
- Uses decent software with nice features
- Available to use free of charge in the lab

## Magspoof

- Handheld device
- Can emulate a card swipe
- Can brute force cards
- Can store many cards in memory
- Sometimes supports all 3 tracks
- Very cheap to build

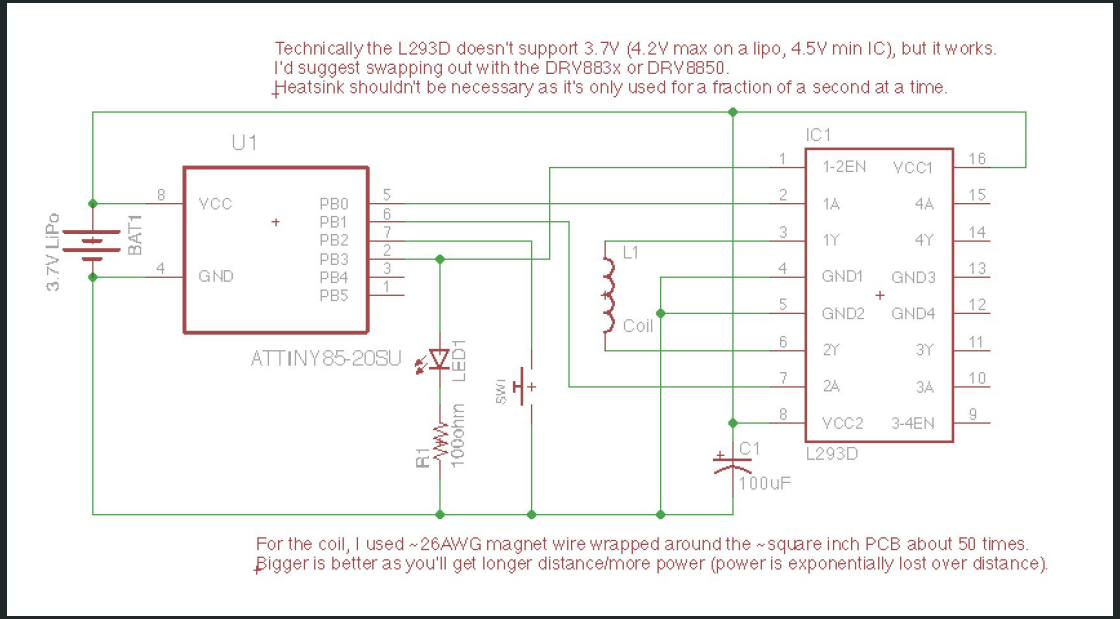
# How does Magspoof work?

# How does Magspoof work?

- Normally, when a card is swiped the sensor reads the track of magnets on the card as they go by.
- Magspoof just turns on and off an electromagnet to simulate magnets coming and going
- Just hold the electromagnet up to a normal card reader.  No RFID, NFC, or Apple pay needed

# Magspoof Parts

- Battery
- Electromagnet
- Motor driver
- Microcontroller



# Who do we have to thank?

- Samy Kamkar
- He single handedly wrote the open source Magspoof code and generously shared his research on his website.
- Check out his website.  I highly recommend it.

# Live Demonstration

- Demonstration of a Magspoof Device

# So, what do we attack?

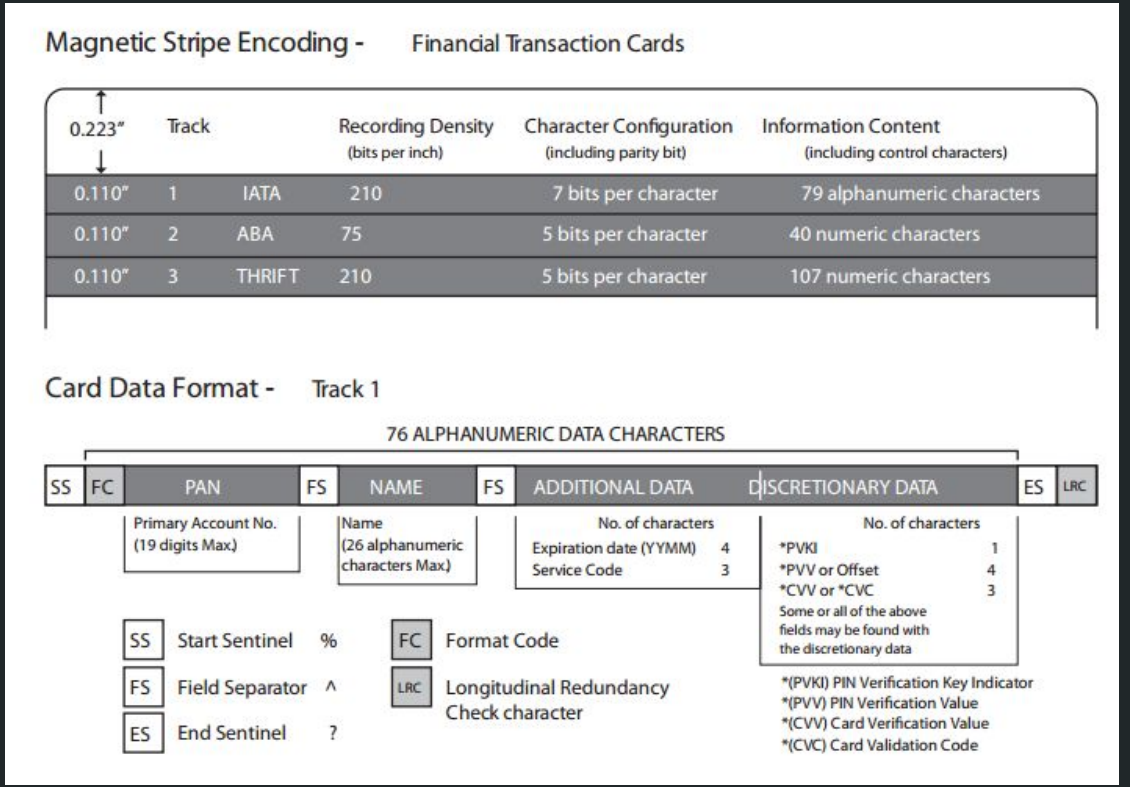
Just about anything...

- Credit/Debit Cards
- Identification Cards
- Security Access Cards
- Parking Garage Cards
- Hotel Keys
- Metro Cards
- Gift Cards
- Etc...

# Credit/Debit Cards

The data on a credit/debit card is as follows

- Card #
- Your Name
- Expiration Date
- Service Code
- Discretionary Data



# Let’s commit credit fraud!

To make a physical copy of a credit/debit card you must have ALL of the data.

1. Obtain Credit Card from target
2. Copy card using MSR605 or use Magspoof to emulate that card
3. Profit… literally

But, wait. Don’t credit cards these days have that chip thing?

- Yep, chip cards have an encrypted chip inside that are pretty hard to beat.

I guess that’s game over…

# Nah, let’s just avoid it

With Amex credit cards Samy Kamkar found a way to completely disable chip.

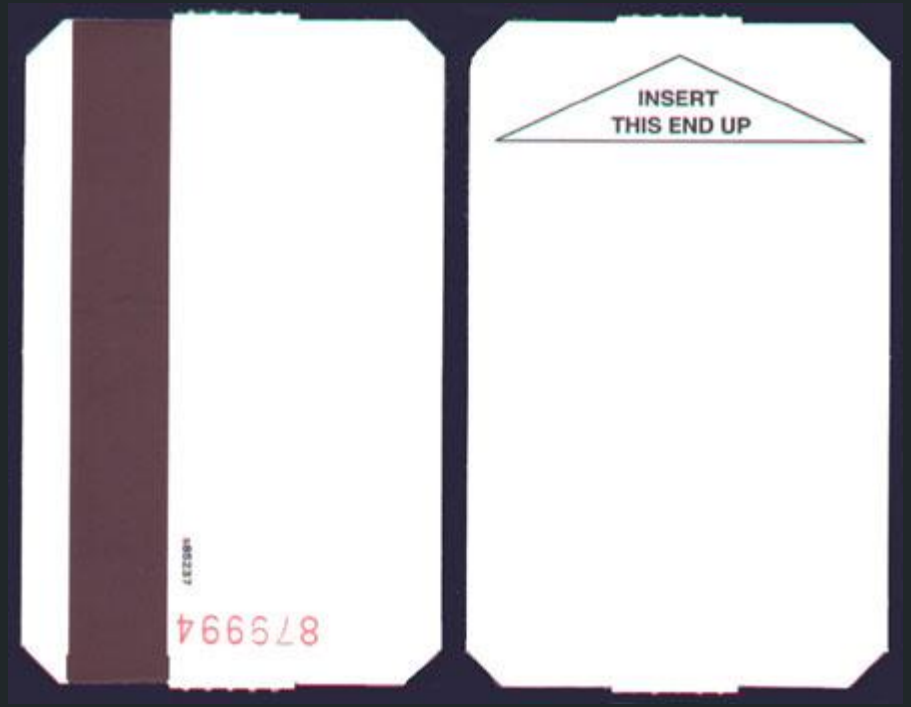
The Service Code states if the card has a chip. Change the service code to state the card has no chip.

The CVV acts as a checksum so, changing the Service Code will change the CVV, but Samy found out that CVV codes from old cards will still get approved.

Just like that, you have disabled chip and are ready to commit credit fraud :)

# Parking Cards

- Using the MSR605 you can change the data on a parking card.
- Most parking lots use different types of cards so, it won't work everywhere...
- But, the idea is to change the data so the machine thinks you are leaving 5 minutes after you came in. Staying in the garage for that little time is free



# Hotel Keys

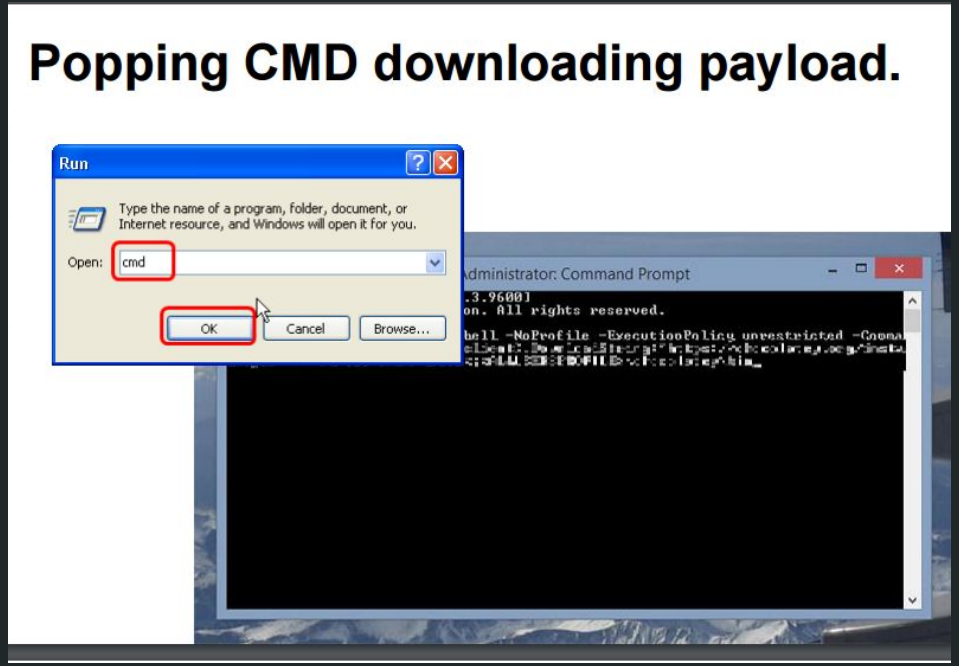
- Hotel Keys usually contain the check out date, room number, and portfolio number
- You should know the room number of the room you're breaking into
- Guess the checkout date
- Brute force the portfolio number
- Boom, you just used Magspoof to breaking into a hotel room

# Keyboard Readers

- Some keyboards have magstripe readers
- These keyboards can accept keyboard key presses through certain magstripe cards...

# Pop a CMD

- Using the keyboard magstripe reader to enter keyboard commands you can open a CMD...
- The possibilities get pretty endless from here...
- Keylogger, data stealing, backdoors...



# Thanks, Weston Hecker

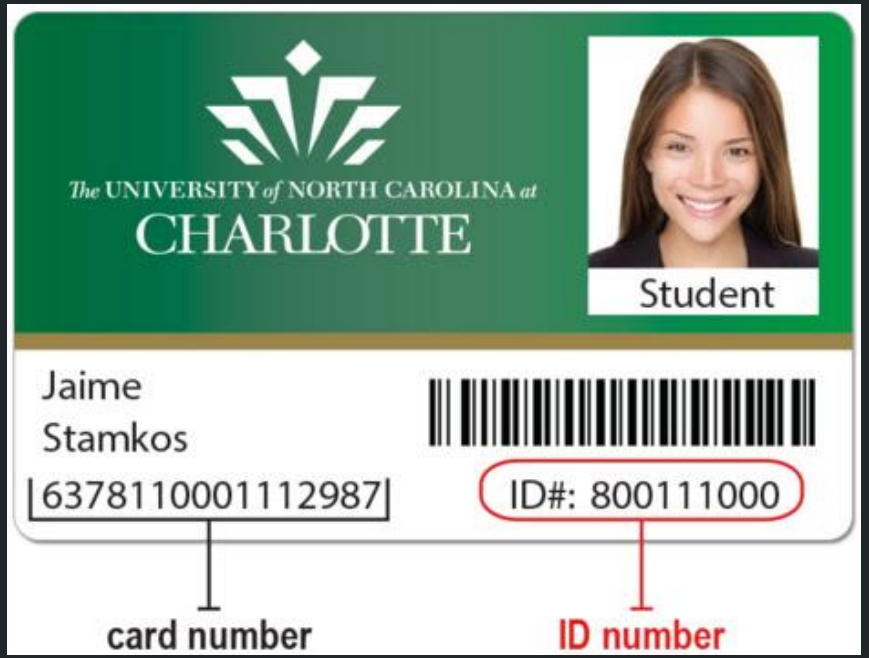
- Weston Hecker saw the concept of Magspoof and took it pretty far.
- He is responsible for the research on hotel key brute forcing and Magstripe keyboard attacking
- His Defcon talk was really interesting

# Let’s steal a UNCC ID

- For real, let’s steal a UNCC ID right now.  This is a live demo.

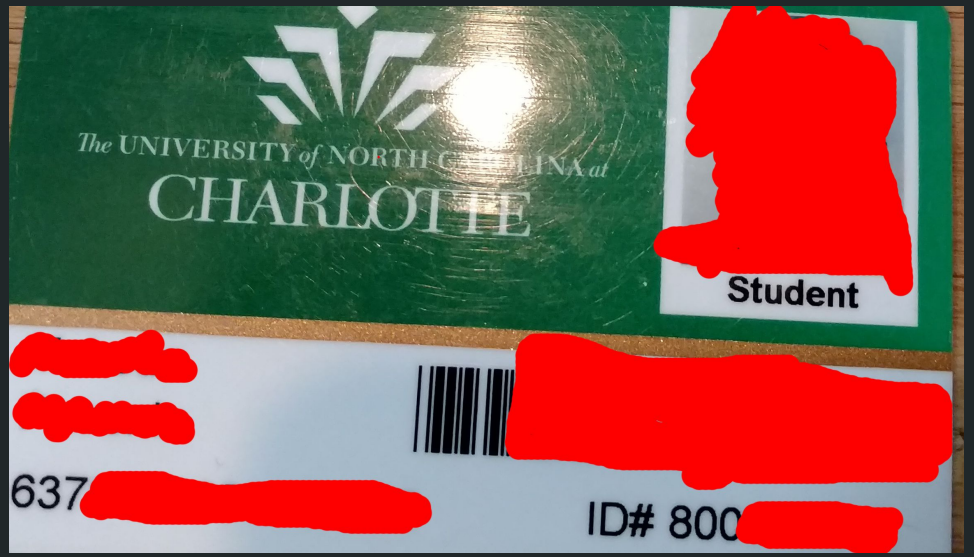
# What Data is on a UNCC ID?

- The old IDs from before last Spring Semester only contained an 800 number and some other data.
- The new IDs contain an 800 number on track 1 and a “card number” (ISO) on track 2.
- This information is also visibly printed on the card, so you can steal the card just by looking at it.



# Getting the Data

- A friend gave me this picture to use for this presentation.
- It probably wouldn't be too hard to get a picture like this without the person knowing.
- Or just get them to swipe their card somewhere where you can see the data
- Now we just copy the "Card Number" and 800 number into the MSR software...



# Making the Copy

- Live demo in progress...

# Implications

- UNCC IDs give access to buildings, identify individuals, and can be used to pay for things.
- It shouldn't be this easy to copy an ID.

# Implications

- The Biology Labs use UNCC IDs to give lab access.  I asked someone in the lab how bad it would be if someone had unauthorized access...
- “The biological material here can be used to make “super bug” weapons. All staff must go through biosafety training up to level 2 to enter the labs.”
- I’m sure no other university has IDs like this...

# Implications

- Chapel Hill also prints the Magstripe data on the outside of the card...

# To learn more...

- The MSR605 card reader is available for use in the 49th SD Lab.
- You can make your own Magpoof with the information below

Useful Links...

Samy's Magspoof Research

Magspoof GitHub

Wikipedia on Magstripe Cards

Weston’s Defcon Talk

# Make your Own Card

Here is some of what you can do...

- Copy an existing card you own (Credit Card, Student ID, Etc)
- Read the data from a card you own
- Add a text string of your choice to a blank card (Think of it as a way to hide data)
- A card Printer may or may not be available