Magnetic Stripe Technology and Beyond

Contents

Chapter 1) About the Author

Author: oooOO Count Zero OOooo

Notice: Restricted Data Transmissions
Date: November 22, 1992

1.1) Disclaimer

Use this info to EXPLORE, not to EXPLOIT. This text is presented for informational purposes only, and I cannot be held responsible for anything you do or any consequences thereof. I do not condone fraud, larceny, or any other criminal activities.

1.2) A Warning

Lately, I've noticed a few "books" and "magazines" for sale that were FILLED with FILES on a variety of computer topics. These file were originally released into the Net with the intention of distributing them for FREE. HOWEVER, these files are now being PACKAGED and sold FOR

PROFIT. This really pisses me off. I am writing this to be SHARED for FREE, and I ask no payment. Feel free to reprint this in hardcopy format and sell it if you must, but NO PROFITS must be made. Not a fucking DIME! If ANYONE reprints this file and tries to sell it FOR A PROFIT, I will hunt you down and make your life miserable. How? Use your imagination. The reality will be worse.

Chapter 2) Introduction

Look in your wallet. Chances are you own at least 3 cards that have magnetic stripes on the back. ATM cards, credit cards, calling cards, frequent flyer cards, ID cards, passcards,...cards, cards, cards! And chances are you have NO idea what information is on those stripes or how they are encoded. This detailed document will enlighten you and hopefully spark your interest in this fascinating field. None of this info is "illegal"...but MANY organizations (the government, credit card companies, security firms, etc.) would rather keep you in the dark. Also, many people will IMMEDIATELY assume that you are a CRIMINAL if you merely "mention" that you are "interested in how magnetic stripe cards work." Watch yourself, ok? Just remember that there is nothing wrong with wanting to know how things work, although in our present society, you may be labelled a "deviant" (or worse, a "hacker")!

Anyway, I will explain in detail how magstripes are encoded and give several examples of the data found on some common cards. I will also cover the technical theory behind magnetic encoding, and discuss magnetic encoding alternatives to magstripes (Wiegand, barium ferrite). Non-magnetic card technology (bar code, infrared, etc.) will be described. Finally, there will be an end discussion on security systems and the ramifications of emergent "smartcard" and biometric technologies.

Chapter 3) Magstripe Fields, Heads, Encoding/Reading

Now, I'll get down to business!

First, I am going to explain the basics behind fields, heads, encoding and reading. Try and absorb the THEORY behind encoding/reading. This will help you greatly if you ever decide to build your own encoder/reader from scratch (more on that later). FERROMAGNETIC materials are substances that retain magnetism after an external magnetizing field is removed. This principle is the basis of ALL magnetic recording and playback. Magnetic POLES always occur in pairs within magnetized material, and MAGNETIC FLUX lines emerge from the NORTH pole and terminate at the SOUTH. The elemental parts of MAGSTRIPES are ferromagnetic particles about 20 millionths of an inch long, each of which acts like a tiny bar magnet. These particles are rigidly held together by a resin binder. The magnetic particles are made by companies which make coloring pigments for the paint industry, and are usually called pigments. When making the magstripe media, the elemental magnetic particles are aligned with their North-South axes parallel to the magnetic stripe by means of an external magnetic fields while the binder hardens.

These particles are actually permanent bar magnets with TWO STABLE POLARITIES. If a magnetic particle is placed in a strong external magnetic field of the opposite polarity, it will

FLIP its own polarity (North becomes South, South becomes North). The external magnetic field strength required to produce this flip is called the COERCIVE FORCE, or COERCIVITY of the particle. Magnetic pigments are available in a variety of coercivities (more on that later on).

An unencoded magstripe is actually a series of North-South magnetic domains (see Figure 1). The adjacent N-S fluxes merge, and the entire stripe acts as a single bar magnet with North and South poles at its ends.

```
Figure 1:               N-S.N-S.N-S.N-S.N-S.N-S.N-S.N-S.N-S <-particles in stripe
---------
       represented as-> N----------------------------S
```

However, if a S-S interface is created somewhere on the stripe, the fluxes will REPEL, and we get a concentration of flux lines around the S-S interface (same with N-N interface). ENCODING consists of creating S-S and N-N interfaces, and READING consists of (you guessed it) detecting 'em. The S-S and N-N interfaces are called FLUX REVERSALS.

```
                            ||| ||| <-flux lines
Figure 2:      N------------N-N-S-S-----------------S
---------     flux lines -> ||| |||
```

The external magnetic field used to flip the polarities is produced by a SOLENOID, which can REVERSE its polarity by reversing the direction of CURRENT. An ENCODING head solenoid looks like a bar magnet bent into the shape of a ring so that the North/South poles are very close and face each other across a tiny gap. The field of the solenoid is concentrated across this gap, and when elemental magnetic particles of the magstripe are exposed to this field, they polarize to the OPPOSITE (unlike poles attract). Movement of the stripe past the solenoid gap during which the polarity of the solenoid is REVERSED will produce a SINGLE flux reversal (see Figure 3). To erase a magstripe, the encoding head is held at a CONSTANT polarity and the ENTIRE stripe is moved past it. No flux reversals, no data.

```
                               | |  <----wires leading to solenoid
                               | |       (wrapped around ring)
                              /-|-|-\
                             /       \
Figure 3:                    |       | <----solenoid (has JUST changed
polarity)

---------                    \       /
                              \ N S / <---gap in ring.. NS polarity across gap
      N----------------------SS-N------------------------S
                              ^^
                  <<<<-direction of stripe movement

          S-S flux reversal created at trailing edge of solenoid!
```

So, we now know that flux reversals are only created the INSTANT the solenoid CHANGES its POLARITY. If the solenoid in Figure 3 were to remain at its current polarity, no further flux reversals would be created as the magstripe moves from right to left. But, if we were to change the solenoid gap polarity >from NS to *SN*, then (you guessed it) a *N-N* flux reversal would

instantly be created. Just remember, for each and every reversal in solenoid polarity, a single flux reversal is created (commit it to memory). An encoded magstripe is therefore just a series of flux reversals (NN followed by SS followed by NN).

DATA! DATA! DATA! That's what you want! How the hell are flux reversals read and interpreted as data? Another solenoid called a READ HEAD is used to detect these flux reversals. The read head operates on the principle of ELECTROMAGNETIC RECIPROCITY: current passing thru a solenoid produces a magnetic field at the gap, therefore, the presence of a magnetic field at the gap of a solenoid coil will **PRODUCE A CURRENT IN THE COIL**! The strongest magnetic fields on a magstripe are at the points of flux reversals. These are detected as voltage peaks by the reader, with +/- voltages corresponding to NN/SS flux reversals (remember, flux reversals come in 2 flavors).

See Figure 4.

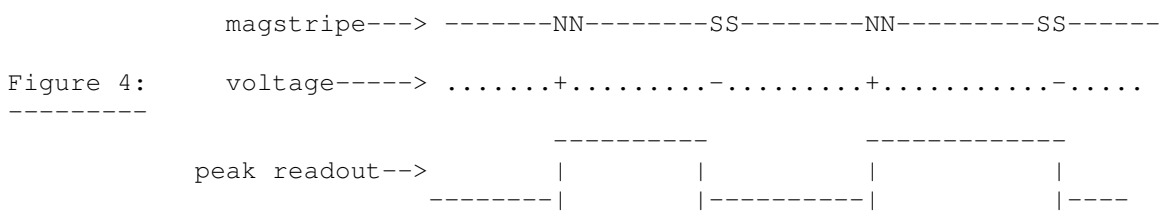


Figure 4:

The "peak readout" square waveform is critical. Notice that the voltage peak remains the same until a new flux reversal is encountered.

Now, how can we encode DATA? The most common technique used is known as Aiken Biphase, or "two-frequency coherent-phase encoding" (sounds impressive, eh?). First, digest the diagrams in Figure 5.

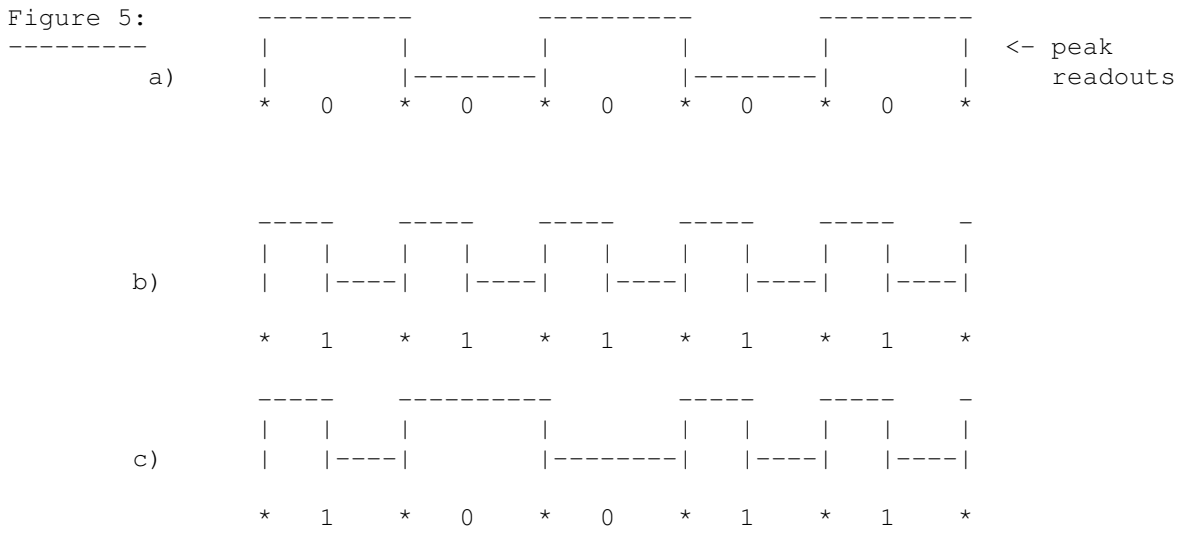


Figure 5:

There you have it. Data is encoded in "bit cells," the frequency of which is the frequency of '0' signals. '1' signals are exactly TWICE the frequency of '0' signals. Therefore, while the actual

frequency of the data passing the read head will vary due to swipe speed, data density, etc, the '1' frequency will ALWAYS be TWICE the '0' frequency. Figure 5C shows exactly how '1' and '0' data exists side by side.

We're getting closer to read DATA! Now, we're all familiar with binary and how numbers and letters can be represented in binary fashion very easily. There are obviously an **INFINITE** number of possible standards, but thankfully the American National Standards Institute (ANSI) and the International Standards Organization (ISO) have chosen 2 standards. The first is

Chapter 4) ANSI/ISO BCD Data format

This is a 5-bit Binary Coded Decimal format. It uses a 16-character set, which uses 4 of the 5 available bits. The 5th bit is an ODD parity bit, which means there must be an odd number of 1's in the 5-bit character..the parity bit will "force" the total to be odd. Also, the Least Significant Bits are read FIRST on the strip. See Figure 6.

The sum of the 1's in each case is odd, thanks to the parity bit. If the read system adds up the 5 bits and gets an EVEN number, it flags the read as ERROR, and you got to scan the card again (I **KNOW** a lot of you out there **ALREADY** understand parity, but I got to cover all the bases...not everyone sleeps with their modem and can recite the entire AT command set at will, you know). See Figure 6 for details of ANSI/ISO BCD.

Figure 6: ANSI/ISO BCD Data Format

- Remember that b1 (bit #1) is the LSB (least significant bit)!
-
- The LSB is read FIRST!
-
- Hexadecimal conversions of the Data Bits are given in parenthesis (xH).
-

--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
```

The magstripe begins with a string of Zero bit-cells to permit the self- clocking feature of biphase to "sync" and begin decoding. A "Start Sentinel" character then tells the reformatting process where to start grouping the decoded bitstream into groups of 5 bits each. At the end of the data, an "End Sentinel" is encountered, which is followed by an "Longitudinal Redundancy Check (LRC) character. The LRC is a parity check for the sums of all b1, b2, b3, and b4 data bits of all preceding characters. The LRC character will catch the remote error that could occur if an individual character had two compensating errors in its bit pattern (which would fool the 5th-bit parity check).

The START SENTINEL, END SENTINEL, and LRC are collectively called "Framing Characters", and are discarded at the end of the reformatting process.

Chapter 5) ANSI/ISO ALPHA Data Format

Alphanumeric data can also be encoded on magstripes. The second ANSI/ISO data format is ALPHA (alphanumeric) and involves a 7-bit character set with 64 characters. As before, an odd parity bit is added to the required 6 data bits for each of the 64 characters. See Figure 7.

Figure 7:
--------- ANSI/ISO ALPHA Data Format

- Remember that b1 (bit #1) is the LSB (least significant bit)!
-
- The LSB is read FIRST!
-
- Hexadecimal conversions of the Data Bits are given in parenthesis (xH).
-

```
  ------Data Bits-------   Parity
  b1  b2  b3  b4  b5  b6     b7    Character   Function

   0   0   0   0   0   0     1      space (0H) Special
```

1	0	0	0	0	0	0	! (1H)	"
0	1	0	0	0	0	0	" (2H)	"
1	1	0	0	0	0	1	# (3H)	"
0	0	1	0	0	0	0	$ (4H)	"
1	0	1	0	0	0	1	% (5H)	Start Sentinel
0	1	1	0	0	0	1	& (6H)	Special
1	1	1	0	0	0	0	' (7H)	"
0	0	0	1	0	0	0	((8H)	"
1	0	0	1	0	0	1	) (9H)	"
0	1	0	1	0	0	1	* (AH)	"
1	1	0	1	0	0	0	+ (BH)	"
0	0	1	1	0	0	1	, (CH)	"
1	0	1	1	0	0	0	- (DH)	"
0	1	1	1	0	0	0	. (EH)	"
1	1	1	1	0	0	1	/ (FH)	"
0	0	0	0	1	0	0	0 (10H)	Data (numeric)
1	0	0	0	1	0	1	1 (11H)	"
0	1	0	0	1	0	1	2 (12H)	"
1	1	0	0	1	0	0	3 (13H)	"
0	0	1	0	1	0	1	4 (14H)	"
1	0	1	0	1	0	0	5 (15H)	"
0	1	1	0	1	0	0	6 (16H)	"
1	1	1	0	1	0	1	7 (17H)	"
0	0	0	1	1	0	1	8 (18H)	"
1	0	0	1	1	0	0	9 (19H)	"
0	1	0	1	1	0	0	: (1AH)	Special
1	1	0	1	1	0	1	; (1BH)	"
0	0	1	1	1	0	0	< (1CH)	"
1	0	1	1	1	0	1	= (1DH)	"
0	1	1	1	1	0	1	> (1EH)	"
1	1	1	1	1	0	0	? (1FH)	End Sentinel
0	0	0	0	0	1	0	@ (20H)	Special
1	0	0	0	0	1	1	A (21H)	Data (alpha)
0	1	0	0	0	1	1	B (22H)	"
1	1	0	0	0	1	0	C (23H)	"
0	0	1	0	0	1	1	D (24H)	"
1	0	1	0	0	1	0	E (25H)	"
0	1	1	0	0	1	0	F (26H)	"
1	1	1	0	0	1	1	G (27H)	"
0	0	0	1	0	1	1	H (28H)	"
1	0	0	1	0	1	0	I (29H)	"
0	1	0	1	0	1	0	J (2AH)	"
1	1	0	1	0	1	1	K (2BH)	"
0	0	1	1	0	1	0	L (2CH)	"
1	0	1	1	0	1	1	M (2DH)	"
0	1	1	1	0	1	1	N (2EH)	"
1	1	1	1	0	1	0	O (2FH)	"
0	0	0	0	1	1	1	(30H)	"
1	0	0	0	1	1	0	Q (31H)	"
0	1	0	0	1	1	0	R (32H)	"
1	1	0	0	1	1	1	S (33H)	"
0	0	1	0	1	1	0	T (34H)	"
1	0	1	0	1	1	1	U (35H)	"
0	1	1	0	1	1	1	V (36H)	"

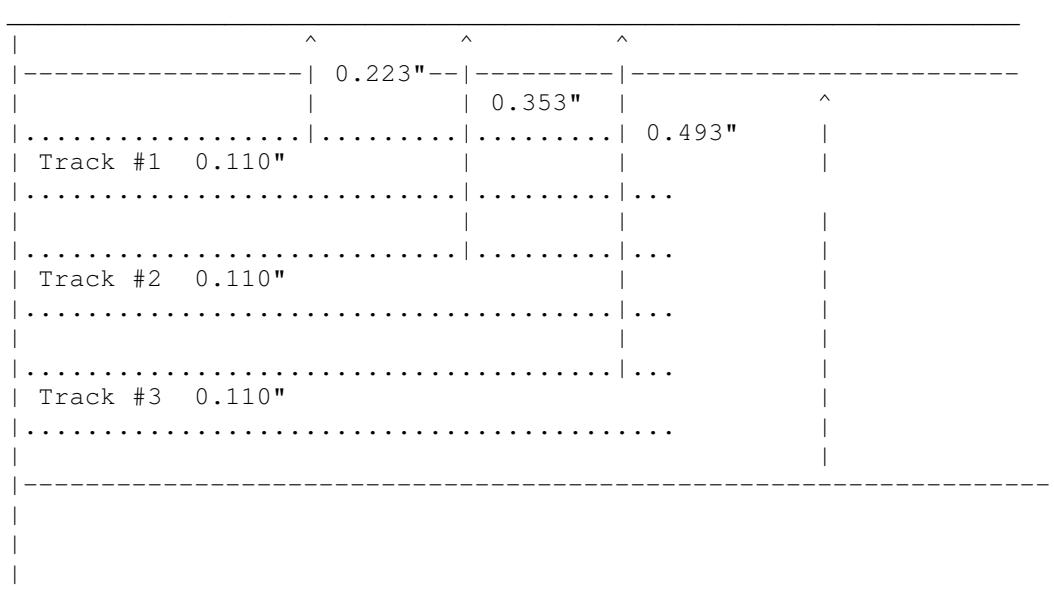
```
1   1   1   0   1   1     0        W (37H)     "
0   0   0   1   1   1     0        X (38H)     "
1   0   0   1   1   1     1        Y (39H)     "
0   1   0   1   1   1     1        Z (3AH)     "

1   1   0   1   1   1     0        [ (3BH)     Special
0   0   1   1   1   1     1        \ (3DH)     Special
1   0   1   1   1   1     0        ] (3EH)     Special
0   1   1   1   1   1     0        ^ (3FH)     Field Separator
1   1   1   1   1   1     1        _ (40H)     Special

    ***** 64 Character 7-bit Set *****
        * 43 Alphanumeric Data Characters
        * 3 Framing/Field Characters
        * 18 Control/Special Characters
```

The two ANSI/ISO formats, ALPHA and BCD, allow a great variety of data to be stored on magstripes. Most cards with magstripes use these formats, but occasionally some do not. More about those later on.

Chapter 6) Tracks and Encoding Protocols

Now we know how the data is stored. But WHERE is the data stored on the magstripe? ANSI/ISO standards define **3** Tracks, each of which is used for different purposes. These Tracks are defined only by their location on the magstripe, since the magstripe as a whole is magnetically homogeneous. See Figure 8.

Figure 8:



You can see the exact distances of each track from the edge of the card, as well as the uniform width and spacing. Place a magstripe card in front of you with the magstripe visible at the bottom of the card. Data is encoded from left to right (just like reading a book). See Figure 9.

Figure 9:
--------- ANSI/ISO Track 1,2,3 Standards

Track	Name	Density	Format	Characters	Function
1	IATA	210 bpi	ALPHA	79	Read Name & Account
2	ABA	75 bpi	BCD	40	Read Account
3	THRIFT	210 bpi	BCD	107	Read Account && *Encode* Transaction

*** Track 1 Layout: ***

SS	FC	PAN	Name	FS	Additional Data	ES	LRC

SS=Start Sentinel "%"
FC=Format Code
PAN=Primary Acct. # (19 digits max)
FS=Field Separator "^"
Name=26 alphanumeric characters max.
Additional Data=Expiration Date, offset, encrypted PIN, etc.
ES=End Sentinel "?"
LRC=Longitudinal Redundancy Check

*** Track 2 Layout: ***

SS	PAN	FS	Additional Data	ES	LRC

SS=Start Sentinel ";"
PAN=Primary Acct. # (19 digits max)
FS=Field Separator "="
Additional Data=Expiration Date, offset, encrypted PIN, etc.
ES=End Sentinel "?"
LRC=Longitudinal Redundancy Check

*** Track 3 Layout: ** Similar to tracks 1 and 2. Almost never used. Many different data standards used.

Track 2, "American Banking Association," (ABA) is most commonly used. This is the track that is read by ATMs and credit card checkers. The ABA designed the specifications of this track and all world banks must abide by it. It contains the cardholder's account, encrypted PIN, plus other discretionary data.

Track 1, named after the "International Air Transport Association," contains the cardholder's name as well as account and other discretionary data. This track is sometimes used by the airlines when securing reservations with a credit card; your name just "pops up" on their machine when they swipe your card!

Since Track 1 can store MUCH more information, credit card companies are trying to urge retailers to buy card readers that read Track 1. The **PROBLEM** is that most card readers read either Track 1 or Track 2, but NOT BOTH! And the installed base of readers currently is biased towards Track 2. VISA USA is at the front of this 'exodus' to Track 1, to the point where they are offering Track 1 readers at reduced prices thru participating banks. A spokesperson for VISA commented:

"We think that Track 1 represents more flexibility and the potential to deliver more information, and we intend to build new services around the increased information." What new services? We can only wait and see.

Track 3 is unique. It was intended to have data read and WRITTEN on it. Cardholders would have account information UPDATED right on the magstripe. Unfortunately, Track 3 is pretty much an orphaned standard. Its **ORIGINAL** design was to control off-line ATM transactions, but since ATMs are now on-line ALL THE TIME, it's pretty much useless. Plus the fact that retailers and banks would have to install NEW card readers to read that track, and that costs $$.

Encoding protocol specifies that each track must begin and end with a length of all Zero bits, called CLOCKING BITS. These are used to synch the self- clocking feature of biphase decoding. See Figure 10.

```
Figure 10:                                end sentinel
                      start sentinel       |  longitudinal redundancy check
                       |                   |  |
      000000000000000 SS.................ES LRC 0000000000000000
       leading           data, data, data           trailing
       clocking bits                                clocking bits
       (length varies)                             (length varies)
```

THAT'S IT!!! There you have the ANSI/ISO STANDARDS! Completely explained. Now, the bad news. NOT EVERY CARD USES IT! Credit cards and ATM cards will follow these standards. BUT, there are many other types of cards out there. Security passes, copy machine cards, ID badges, and EACH of them may use a PROPRIETARY density/format/track-location system. ANSI/ISO is REQUIRED for financial transaction cards used in the international interbank network. All other cards can play their own game.

The good news. MOST other cards follow the standards, because it's EASY to follow a standard instead of WORKING to make your OWN! Most magstripe cards other than credit cards and ATM cards will use the same Track specifications, and use either BCD or ALPHA formats.

Chapter 7) A Bit About Magstripe Equipment

"Wow, now I know how to interpret all that data on magstripes! But.waitasec, what kind of equipment do I need to read the stripes? Where can I buy a reader? I don't see any in Radio Shack!!"

Sorry, but magstripe equipment is hard to come by. For obvious reasons, card readers are not made commonly available to consumers. How to build one is the topic for another file (this file is already too long).

Your best bets are to try and scope out Electronics Surplus Stores and flea markets. Do not even bother trying to buy one directly from a manufacturer, since they will immediately assume you have "criminal motives." And as for getting your hands on a magstripe ENCODER...well, good luck! Those rare beauties are worth their weight in gold. Keep your eyes open and look around, and MAYBE you'll get lucky! A bit of social engineering can go a LONG way.

There are different kinds of magstripe readers/encoders. The most common ones are "swipe" machines: the type you have to physically slide the card thru. Others are "insertion" machines: like ATM machines they 'eat' your card, then regurgitate it after the transaction. Costs are in the thousands of dollars, but like I said, flea markets and surplus stores will often have GREAT deals on these things. Another problem is documentation for these machines. If you call the manufacturer and simply ask for 'em, they will probably deny you the literature. "Hey son, what are you doing with our model XYZ swipe reader? That belongs in the hands of a "qualified" merchant or retailer, not some punk kid trying to "find out how things work!" Again, some social engineering may be required. Tell 'em you're setting up a new business. Tell 'em you're working on a science project. Tell 'em anything that works!

2600 Magazine recently had a good article on how to build a machine that copies magstripe cards. Not much info on the actual data formats and encoding schemes, but the device described is a start. With some modifications, I bet you could route the output to a dumb terminal (or thru a null modem cable) in order to READ the data. Worth checking out the schematics.

As for making your own cards, just paste a length of VCR, reel-to-reel, or audio cassette tape to a cut-out posterboard or plastic card. Works just as good as the real thing, and useful to experiment with if you have no expired or 'dead' ATM or calling cards lying around (SAVE them, don't TOSS them!).

Chapter 8) Examples of Data on Magstripes

The real fun in experimenting with magstripe technology is READING cards to find out WHAT THE HELL is ON them! Haven't you wondered? The following cards are the result of my own 'research'. Data such as specific account numbers and names has been changed to protect the innocent. None the cards used to make this list were stolen or acquired illegally.

Notice that I make careful note of "common data." This is data that I noticed was the same for all cards of a particular type. This is highlighted below the data with asterisks (*). Where I found varying data, I indicate it with "x"'s. In those cases, NUMBER of CHARACTERS was consistent (the number of "x"'s equals the number of characters...one to one relationship).

I still don't know what some of the data fields are for, but hopefully I will be following this file with a sequel after I collect more data. It ISN'T easy to find lots of cards to examine. Ask your friends, family, and co-workers to help! "Hey, can I, ahh, like BORROW your MCI calling card

tonight? I'm working on an, ahh, EXPERIMENT. Please?" Just...be honest! Also, do some trashing. People will often BEND expired cards in half, then throw them out. Simply bend them back into their normal shape, and they'll usually work (I've done it!). They may be expired, but they're not ERASED!

8.1) Mastercard

```
-=Mastercard=-  Number on front of card -> 1111 2222 3333 4444
                Expiration date -> 12/99

Track 2 (BCD,75 bpi)-> ;1111222233334444=99121010000000000000?
                                           ***

Track 1 (ALPHA,210 bpi)-> %B1111222233334444^PUBLIC/JOHN?
                           *
```

Note that the "101" was common to all MC cards checked, as well as the "B".

8.2) VISA

```
-=VISA=-  Number on front of card -> 1111 2222 3333 4444
          Expiration date -> 12/99

Track 2 (BCD,75 bpi)-> ;1111222233334444=9912101xxxxxxxxxxxxx?
                                           ***
Track 1 (ALPHA,210 bpi)->
%B1111222233334444^PUBLIC/JOHN^9912101xxxxxxxxxxxxx?
                           *
```

Note that the "101" was common to all VISA cards checked, as well as the "B". Also, the "xxx" indicates numeric data that varied from card to card, with no apparent pattern. I believe this is the encrypted pin for use when cardholders get 'cash advances' from ATMs. In every case, tho, I found *13* digits of the stuff.

8.3) Discover

```
-=Discover=-  Number on front of card -> 1111 2222 3333 4444
              Expiration date -> 12/99

Track 2 (BCD,75 bpi)-> ;1111222233334444=991210100000?
                                           ********

Track 1 (ALPHA,210 bpi)-> %B1111222233334444^PUBLIC/JOHN___^991210100000?
                                                           ********
```

Note, the "10100000" and "B" were common to most DISCOVER cards checked. I found a few that had "10110000" instead. Don't know the significance. Note the underscores after the name JOHN. I found consistently that the name data field had *26* characters. Whatever was left of the field after the name was "padded" with SPACES. So...for all of you with names longer than 25 (exclude the "/") characters, PREPARE to be TRUNCATED! ;)

8.4) US Sprint FON

```
-=US Sprint FON=-  Number on front of card -> 111 222 3333 4444

Track 2 (BCD,75 bpi)-> ;xxxxxx11122233339==xxx4444xxxxxxxxxx=?
                                          *

Track 1 (ALPHA,210 bpi)-> %B^ /^^xxxxxxxxxxxxxxxx?
                             *
```

Strange. None of the cards I check had names in the Track 1 fields. Track 1 looks unused, yet it was always formatted with field separators. The "xxx" stuff varied from card to card, and I didn't see a pattern. I know it isn't a PIN, so it must be account data.

8.5) Fleet Bank

```
-=Fleet Bank=-  Number on front of card -> 111111 222 3333333
                Expiration date -> 12/99

Track 2 (BCD,75 bpi)-> ;1111112223333333=9912120100000000xxxx?
                                           ****

Track 1 (ALPHA,210 bpi) ->
         %B1111112223333333^PUBLIC/JOHN___^99121201000000000000xxxx000000?
          *                                  ****
```

Note that the "xxx" data varied. This is the encrypted PIN offset. Always 4 digits (hmmm...). The "1201" was always the same. In fact, I tried many ATM cards from DIFFERENT BANKS...and they all had "1201".

8.6) Radio Shack

```
(Can't leave *this* one out ;)
-=Radio Shack=-  Number on front of card -> 1111 222 333333
                 NO EXPIRATION data on card

Track 2 (BCD,75 dpi)-> ;1111222333333=9912101?
                                     *******
```

Note that the "9912101" was the SAME for EVERY Radio Shack card I saw. Looks like when they don't have 'real' data to put in the expiration date field, they have to stick SOMETHING in there.

Well, that's all I'm going to put out right now. As you can see, the major types of cards (ATMs, CC) all follow the same rules more or less. I checked out a number of security passcards and timeclock entry cards..and they ALL had random stuff written to Track 2. Track 2 is by FAR the MOST utilized track on the card. And the format is pretty much always ANSI/ISO BCD. I **DID** run into some hotel room access cards that, when scanned, were GARBLED. They most likely used a character set other than ASCII (if they were audio tones, my reader would have put out NOTHING...as opposed to GARBLED data). As you can see, one could write a BOOK listing

different types of card data. I intended only to give you some examples. My research has been limited, but I tried to make logical conclusions based on the data I received.

Chapter 9) Cards of All Flavors

People wanted to store A LOT of data on plastic cards. And they wanted that data to be 'invisible' to cardholders. Here are the different card technologies that were invented and are available today.

HOLLERITH

With this system, holes are punched in a plastic or paper card and read optically. One of the earliest technologies, it is now seen as an encoded room key in hotels. The technology is not secure, but cards are cheap to make.

BAR CODE

The use of bar codes is limited. They are cheap, but there is virtually no security and the bar code strip can be easily damaged.

INFRARED

Not in widespread use, cards are factory encoded by creating a "shadow pattern" within the card. The card is passed thru a swipe or insertion reader that uses an infrared scanner. Infrared card pricing is moderate to expensive, and encoding is pretty secure. Infrared scanners are optical and therefore vulnerable to contamination.

PROXIMITY

Hands-free operation is the primary selling point of this card. Although several different circuit designs are used, all proximity cards permit the transmission of a code simply by bringing the card near the reader (6-12"). These cards are quite thick, up to 0.15" (the ABA standard is 0.030"!).

WIEGAND

Named after its inventor, this technology uses a series of small diameter wires that, when subjected to a changing magnetic field, induce a discrete voltage output in a sensing coil. Two rows of wires are embedded in a coded strip. When the wires move past the read head, a series of pulses is read and interpreted as binary code. This technology produces cards that are VERY hard to copy or alter, and cards are moderately expensive to make. Readers based on this tech are epoxy filled, making them immune to weather conditions, and neither card nor readers are affected by external magnetic fields (don't worry about leaving these cards on top of the television set...you can't hurt them!). Here's an example of the layout of the wires in a Wiegand strip:

The wires are NOT visible from the outside of the card, but if your card is white, place it in front of a VERY bright light source and peer inside. Notice that the spacings between the wires is uniform.

BARIUM FERRITE

The oldest magnetic encoding technology (been around for 40 yrs!) it uses small bits of magnetized barium ferrite that are placed inside a plastic card. The polarity and location of the "spots" determines the coding. These cards have a short life cycle, and are used EXTENSIVELY in parking lots (high turnover rate, minimal security). Barium Ferrite cards are ONLY used with INSERTION readers.
There you have the most commonly used cards. Magstripes are common because they are CHEAP and relatively secure.

Chapter 10) Magstripe Coercivity

Magstripes themselves come in different flavors. The COERCIVITY of the magnetic media must be specified. The coercivity is the magnetic field strength required to demagnetize an encoded stripe, and therefore determines the encode head field strength required to encode the stripe. A range of media coercivities are available ranging from 300 Oersteds to 4,000 Oe. That boils down to HIGH-ENERGY magstripes (4,000 Oe) and LOW-ENERGY magstripes (300 Oe).

REMEMBER: since all magstripes have the same magnetic remanence regardless of their coercivity, readers CANNOT tell the difference between HIGH and LOW energy stripes. Both are read the same by the same machines.

LOW-ENERGY media is most common. It is used on all financial cards, but its disadvantage is that it is subject to accidental demagnetization from contact with common magnets (refrigerator, TV magnetic fields, etc.). But these cards are kept safe in wallets and purses most of the time.

HIGH-ENERGY media is used for ID Badges and access control cards, which are commonly used in 'hostile' environments (worn on uniform, used in stockrooms). Normal magnets will not affect these cards, and low-energy encoders cannot write to them.

Chapter 11) Not All that Fluxes is Digital

Not all magstripe cards operate on a digital encoding method. SOME cards encode AUDIO TONES, as opposed to digital data. These cards are usually used with old, outdated, industrial-strength equipment where security is not an issue and not a great deal of data need be encoded on the card. Some subway passes are like this. They require only expiration data on the magstripe, and a short series of varying frequencies and durations are enough. Frequencies will vary with the speed of swiping, but RELATIVE frequencies will remain the same (for instance, tone 1 is

twice the freq. of tone 2, and .5 the freq of tone 3, regardless of the original frequencies!). Grab an oscilloscope to visualize the tones, and listen to them on your stereo. I haven't experimented with these types of cards at all.

Chapter 12) Security and Smartcards

Many security systems utilize magstripe cards, in the form of passcards and ID cards. It's interesting, but I found in a NUMBER of cases that there was a serious FLAW in the security of the system. In these cases, there was a code number PRINTED on the card. When scanned, I found this number encoded on the magstripe. Problem was, the CODE NUMBER was ALL I found on the magstripe! Meaning, by just looking at the face of the card, I immediately knew exactly what was encoded on it. Ooops! Makes it pretty damn easy to just glance at Joe's card during lunch, then go home and pop out my OWN copy of Joe's access card! Fortunately, I found this flaw only in 'smaller' companies (sometimes even universities). Bigger companies seem to know better, and DON'T print ALL of the magstripe data right on card in big, easily legible numbers. At least the big companies **I** checked. ;)

Other security blunders include passcard magstripes encoded ONLY with the owner's social security number (yeah, real difficult to find out a person's SS#...GREAT idea), and having passcards with only 3 or 4 digit codes.

Smartcard technology involves the use of chips embedded in plastic cards, with pinouts that temporarily contact the card reader equipment. Obviously, a GREAT deal of data could be stored in this way, and unauthorized duplication would be very difficulty. Interestingly enough, not much effort is being put into smartcards by the major credit card companies. They feel that the tech is too expensive, and that still more data can be squeezed onto magstripe cards in the future (especially Track 1). I find this somewhat analogous to the use of metallic oxide disk media. Sure, it's not the greatest (compared to erasable- writable optical disks), but it's CHEAP..and we just keep improving it. Magstripes will be around for a long time to come. The media will be refined, and data density increased. But for conventional applications, the vast storage capabilities of smartcards are just not needed.

Chapter 13) Biometrics: Throw yer cards away!

I'd like to end with a mention of biometrics: the technology based on reading the physical attributes of an individual thru retina scanning, signature verification, voice verification, and other means. This was once limited to government use and to supersensitive installations. However, biometrics will soon acquire a larger market share in access control sales because much of its development stage has passed and costs will be within reach of more buyers. Eventually, we can expect biometrics to replace pretty much ALL cards..because all those plastic cards in your wallet are there JUST to help COMPANIES **IDENTIFY** YOU. And with biometrics, they'll know you without having to read cards.

I'm not paranoid, nor do I subscribe to any grand "corporate conspiracy," but I find it a bit unsettling that our physical attributes will most likely someday be sitting in the cool, vast

electronic databases of the CORPORATE world. Accessible by anyone willing to pay. Imagine CBI and TRW databases with your retina image, fingerprint, and voice pattern online for instant, convenient retrieval. Today, a person can CHOOSE NOT to own a credit card or a bank card...we can cut up our plastic ID cards! Without a card, a card reader is useless and cannot identify you.

Paying in cash makes you invisible! However, with biometrics, all a machine has to do is watch... listen...and record. With government/corporate America pushing all the buttons. "Are you paying in cash?..Thank you...Please look into the camera. Oh, I see your name is Mr. Smith...uh, oh...my computer tells me you haven't paid your gas bill...afraid I'm going to have to keep this money and credit your gas account with it....do you have any more cash?...or would you rather I garnish your paycheck?" heh heh

Chapter 14) Closing Notes (FINALLY!)

Whew...this was one MOTHER of a file. I hope it was interesting, and I hope you distribute it to all you friends. This file was a production of "Restricted Data Transmissions"...a group of techies based in the Boston area that feel that "Information is Power"...and we intend to release a number of highly technical yet entertaining files in the coming year....LOOK FOR THEM!! Tomorrow I'm on my way to Xmascon '91... we made some slick buttons commemorating the event...if you ever see one of them (green wreath.XMASCON 1991 printed on it).hang on to it!... it's a collector's item.. (hahahah) Boy, I'm sleepy...

Remember.... "Truth is cheap, but information costs!"
But -=RDT is gonna change all that... ;) set the info FREE!
Peace.

Chapter 15) Greets

..oooOO Count Zero OOooo..

Usual greets to Magic Man, Brian Oblivion, Omega, White Knight, and anyone else I ever bummed a cigarette off.

(1/18/92 addition: Greets to everyone I met at Xmascon..including but not excluding Crimson Death, Dispater, Sterling, Mack Hammer, Erik Bloodaxe, Holistic Hacker, Pain Hertz, Swamp Ratte, G.A.Ellsworth, Phaedrus, Moebius, Lord MacDuff, Judge Dredd, and of course hats off to *Drunkfux* for organizing and taking responsibility for the whole damn thing. Hope to see all of you at SummerCon '92! Look for Cyber-striper GIFs at a BBS near you..heh heh)

Comments, criticisms, and discussions about this file are welcome. I can be reached at:

- count0@world.std.com
- count0@spica.bu.edu
- count0@atdt.org

Magic Man and I are the sysops of the BBS "ATDT"...located somewhere in Massachusetts. Great message bases, technical discussions...data made flesh...electronic underground.....our own Internet address (atdt.org)... field trips to the tunnels under MIT in Cambridge.....give it a call.. mail me for more info.. ;)