<?xml version="1.0" encoding="utf-8" ?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">

<head>

<meta http-equiv="content-type" content="text/html; charset=utf-8" />

<meta http-equiv="content-language" content="en" />

<meta name="description" content="Phrack staff website." />

<meta name="keywords" content="phrack" />

<meta name="robots" content="follow,index,all" />

<meta name="revisit-after" content="7 days" />

<title>.:: Phrack Magazine ::.</title>

<link href="../../css/style.css" rel="stylesheet" type="text/css">

</head>

<body id="top">

<div align="center" class="texto-2-bold">

[ <a href="../../index.html" title="News">News</a> ]

[ <a href="../../papers/shockwave\_memory\_disclosure.html" title="Paper Feed">Paper Feed</a> ]

[ <a href="../../issues/68/1.html" title="Issues">Issues</a> ]

[ <a href="../../authors.html" title="Authors">Authors</a> ]

[ <a href="../../archives/" title="Archives">Archives</a> ]

[ <a href="../../contact.html" title="Contact">Contact</a> ]

</div>

<center>

<br>

<br>

<img width="600" src="../../images/phrack-logo.jpg" alt="..[ Phrack Magazine ]..">

<br>

<div class="texto-2">

<div class="p-title">.:: Card-O-Rama: Magnetic Stripe Technology and Beyond ::.</div>

<hr width="600" />

</div>

<div style="padding-top: 4px; padding-bottom: 4px;">

<div class="around">

<div class="details"><strong>Issues</strong>:

[ <a href="../../issues/1/1.html" title="Issue 1">1</a> ] [ <a href="../../issues/2/1.html" title="Issue 2">2</a> ] [ <a href="../../issues/3/1.html" title="Issue 3">3</a> ] [ <a href="../../issues/4/1.html" title="Issue 4">4</a> ] [ <a href="../../issues/5/1.html" title="Issue 5">5</a> ] [ <a href="../../issues/6/1.html" title="Issue 6">6</a> ] [ <a href="../../issues/7/1.html" title="Issue 7">7</a> ] [ <a href="../../issues/8/1.html" title="Issue 8">8</a> ] [ <a href="../../issues/9/1.html" title="Issue 9">9</a> ] [ <a href="../../issues/10/1.html" title="Issue 10">10</a> ] [ <a href="../../issues/11/1.html" title="Issue 11">11</a> ] [ <a href="../../issues/12/1.html" title="Issue 12">12</a> ] [ <a href="../../issues/13/1.html" title="Issue 13">13</a> ] [ <a href="../../issues/14/1.html" title="Issue 14">14</a> ] [ <a href="../../issues/15/1.html" title="Issue 15">15</a> ] [ <a href="../../issues/16/1.html" title="Issue 16">16</a> ] [ <a href="../../issues/17/1.html" title="Issue 17">17</a> ] [ <a href="../../issues/18/1.html" title="Issue 18">18</a> ] [ <a href="../../issues/19/1.html" title="Issue 19">19</a> ] [ <a href="../../issues/20/1.html" title="Issue 20">20</a> ] [ <a href="../../issues/21/1.html" title="Issue 21">21</a> ] [ <a href="../../issues/22/1.html" title="Issue 22">22</a> ] [ <a href="../../issues/23/1.html" title="Issue 23">23</a> ] [ <a href="../../issues/24/1.html" title="Issue 24">24</a> ] [ <a href="../../issues/25/1.html" title="Issue 25">25</a> ] [ <a href="../../issues/26/1.html" title="Issue 26">26</a> ] [ <a href="../../issues/27/1.html" title="Issue 27">27</a> ] [ <a href="../../issues/28/1.html" title="Issue 28">28</a> ] [ <a href="../../issues/29/1.html" title="Issue 29">29</a> ] [ <a href="../../issues/30/1.html" title="Issue 30">30</a> ] [ <a href="../../issues/31/1.html" title="Issue 31">31</a> ] [ <a href="../../issues/32/1.html" title="Issue 32">32</a> ] [ <a href="../../issues/33/1.html" title="Issue 33">33</a> ] [ <a href="../../issues/34/1.html" title="Issue 34">34</a> ] [ <a href="../../issues/35/1.html" title="Issue 35">35</a> ] [ <a href="../../issues/36/1.html" title="Issue 36">36</a> ] [ <a class="current" href="../../issues/37/1.html" title="Issue 37">37</a> ] [ <a href="../../issues/38/1.html" title="Issue 38">38</a> ] [ <a href="../../issues/39/1.html" title="Issue 39">39</a> ] [ <a href="../../issues/40/1.html" title="Issue 40">40</a> ] [ <a href="../../issues/41/1.html" title="Issue 41">41</a> ] [ <a href="../../issues/42/1.html" title="Issue 42">42</a> ] [ <a href="../../issues/43/1.html" title="Issue 43">43</a> ] [ <a href="../../issues/44/1.html" title="Issue 44">44</a> ] [ <a href="../../issues/45/1.html" title="Issue 45">45</a> ] [ <a href="../../issues/46/1.html" title="Issue 46">46</a> ] [ <a href="../../issues/47/1.html" title="Issue 47">47</a> ] [ <a href="../../issues/48/1.html" title="Issue 48">48</a> ] [ <a href="../../issues/49/1.html" title="Issue 49">49</a> ] [ <a href="../../issues/50/1.html" title="Issue 50">50</a> ] [ <a href="../../issues/51/1.html" title="Issue 51">51</a> ] [ <a href="../../issues/52/1.html" title="Issue 52">52</a> ] [ <a href="../../issues/53/1.html" title="Issue 53">53</a> ] [ <a href="../../issues/54/1.html" title="Issue 54">54</a> ] [ <a href="../../issues/55/1.html" title="Issue 55">55</a> ] [ <a href="../../issues/56/1.html" title="Issue 56">56</a> ] [ <a href="../../issues/57/1.html" title="Issue 57">57</a> ] [ <a href="../../issues/58/1.html" title="Issue 58">58</a> ] [ <a href="../../issues/59/1.html" title="Issue 59">59</a> ] [ <a href="../../issues/60/1.html" title="Issue 60">60</a> ] [ <a href="../../issues/61/1.html" title="Issue 61">61</a> ] [ <a href="../../issues/62/1.html" title="Issue 62">62</a> ] [ <a href="../../issues/63/1.html" title="Issue 63">63</a> ] [ <a href="../../issues/64/1.html" title="Issue 64">64</a> ] [ <a href="../../issues/65/1.html" title="Issue 65">65</a> ] [ <a href="../../issues/66/1.html" title="Issue 66">66</a> ] [ <a href="../../issues/67/1.html" title="Issue 67">67</a> ] [ <a href="../../issues/68/1.html" title="Issue 68">68</a> ]

</div>

<div class="opt" align="center"><div class="rt"><a href="../../archives/tgz/phrack37.tar.gz" title="Get current issue tar.gz">Get tar.gz</a></div><strong>Current issue</strong> : #<a href="../../archives/tgz/phrack37.tar.gz" title="Get current issue tar.gz">37</a> | <strong>Release date</strong> : <b>1992-01-03</b> | <strong>Editor</strong> : <b>Dispater</b></div>

<div style="border-top: 1px solid black; border-bottom: 2px solid black">

<table class="tissue" cellpadding="0" cellspacing="0">

<tbody>

<tr><td align="left"><a href="../../issues/37/1.html#article">Introduction</a></td><td align="right">Dispater</td></tr>

<tr><td align="left"><a href="../../issues/37/2.html#article">Phrack Loopback</a></td><td align="right">Phrack Staff</td></tr>

<tr><td align="left"><a href="../../issues/37/3.html#article">Pirate's Cove</a></td><td align="right">Rambone</td></tr>

<tr><td align="left"><a href="../../issues/37/4.html#article">Exploring Information-America</a></td><td align="right">White Knight &amp; The Omega</td></tr>

<tr><td align="left"><a href="../../issues/37/5.html#article">Beating The Radar Rap Part 1 of 2</a></td><td align="right">Dispater</td></tr>

<tr><td align="left"><a href="../../issues/37/6.html#article">Card-O-Rama: Magnetic Stripe Technology and Beyond</a></td><td align="right">Count Zero</td></tr>

<tr><td align="left"><a href="../../issues/37/7.html#article">Users Guide to VAX/VMS Part 2 of 3</a></td><td align="right">Black Kat</td></tr>

<tr><td align="left"><a href="../../issues/37/8.html#article">Basic Commands for the VOS System</a></td><td align="right">Dr. No-Good</td></tr>

<tr><td align="left"><a href="../../issues/37/9.html#article">The CompuServe Case</a></td><td align="right">EFF</td></tr>

<tr><td align="left"><a href="../../issues/37/10.html#article">PWN Special Report VI on WeenieFest '92</a></td><td align="right">Count Zero</td></tr>

<tr><td align="left"><a href="../../issues/37/11.html#article">PWN/Part 1</a></td><td align="right">Spirit Walker</td></tr>

<tr><td align="left"><a href="../../issues/37/12.html#article">PWN/Part 2</a></td><td align="right">Spirit Walker</td></tr>

<tr><td align="left"><a href="../../issues/37/13.html#article">PWN/Part 3</a></td><td align="right">Spirit Walker</td></tr>

<tr><td align="left"><a href="../../issues/37/14.html#article">PWN/Part 4</a></td><td align="right">Spirit Walker</td></tr>

</tbody>

</table>

<div class="opt" id="article"><strong>Title</strong> : Card-O-Rama: Magnetic Stripe Technology and Beyond</div>

<div class="opt-bottom"> <strong>Author</strong> : Count Zero</div>

<pre> Card-O-Rama: Magnetic Stripe Technology and Beyond

or

&quot;A Day in the Life of a Flux Reversal&quot;

Written by

oooOO Count Zero OOooo

Restricted Data Transmissions

November 22, 1992

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 &quot;illegal&quot;...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 &quot;mention&quot; that you are &quot;interested in how magnetic

stripe cards work.&quot; 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 &quot;deviant&quot; (or worse, &lt;gasp&gt; a &quot;hacker&quot;)!

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

&quot;smartcard&quot; and biometric technologies.

\*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.

\*A WARNING\*

Lately, I've noticed a few &quot;books&quot; and &quot;magazines&quot; 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.

\*\* 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 &lt;-particles in stripe

---------

represented as-&gt; 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.

||| ||| &lt;-flux lines

Figure 2: N------------N-N-S-S-----------------S

--------- flux lines -&gt; ||| |||

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.

| | &lt;----wires leading to solenoid

| | (wrapped around ring)

/-|-|-\

/ \

Figure 3: | | &lt;----solenoid (has JUST changed polarity)

--------- \ /

\ N S / &lt;---gap in ring.. NS polarity across gap

N----------------------SS-N-------------------------S

^^

&lt;&lt;&lt;&lt;&lt;-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

&gt;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.

magstripe---&gt; -------NN--------SS--------NN---------SS------

Figure 4: voltage-----&gt; .......+.........-.........+...........-.....

---------

---------- -------------

peak readout--&gt; | | | |

--------| |----------| |----

The &quot;peak readout&quot; 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 &quot;two-frequency coherent-phase encoding&quot; (sounds impressive,

eh?). First, digest the diagrams in Figure 5.

Figure 5: ---------- ---------- ----------

--------- | | | | | | &lt;- peak

a) | |--------| |--------| | readouts

\* 0 \* 0 \* 0 \* 0 \* 0 \*

----- ----- ----- ----- ----- -

| | | | | | | | | | |

b) | |----| |----| |----| |----| |----|

\* 1 \* 1 \* 1 \* 1 \* 1 \*

----- ---------- ----- ----- -

| | | | | | | | |

c) | |----| |--------| |----| |----|

\* 1 \* 0 \* 0 \* 1 \* 1 \*

There you have it. Data is encoded in &quot;bit cells,&quot; 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

\*\* 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

&quot;force&quot; 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) &quot;

0 1 0 0 0 2 (2H) &quot;

1 1 0 0 1 3 (3H) &quot;

0 0 1 0 0 4 (4H) &quot;

1 0 1 0 1 5 (5H) &quot;

0 1 1 0 1 6 (6H) &quot;

1 1 1 0 0 7 (7H) &quot;

0 0 0 1 0 8 (8H) &quot;

1 0 0 1 1 9 (9H) &quot;

0 1 0 1 1 : (AH) Control

1 1 0 1 0 ; (BH) Start Sentinel

0 0 1 1 1 &lt; (CH) Control

1 0 1 1 0 = (DH) Field Separator

0 1 1 1 0 &gt; (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 &quot;sync&quot; and begin decoding. A &quot;Start Sentinel&quot;

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 &quot;End

Sentinel&quot; is encountered, which is followed by an &quot;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 &quot;Framing

Characters&quot;, and are discarded at the end of the reformatting process.

\*\* 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) &quot;

0 1 0 0 0 0 0 &quot; (2H) &quot;

1 1 0 0 0 0 1 # (3H) &quot;

0 0 1 0 0 0 0 $ (4H) &quot;

1 0 1 0 0 0 1 % (5H) Start Sentinel

0 1 1 0 0 0 1 &amp; (6H) Special

1 1 1 0 0 0 0 ' (7H) &quot;

0 0 0 1 0 0 0 ( (8H) &quot;

1 0 0 1 0 0 1 ) (9H) &quot;

0 1 0 1 0 0 1 \* (AH) &quot;

1 1 0 1 0 0 0 + (BH) &quot;

0 0 1 1 0 0 1 , (CH) &quot;

1 0 1 1 0 0 0 - (DH) &quot;

0 1 1 1 0 0 0 . (EH) &quot;

1 1 1 1 0 0 1 / (FH) &quot;

0 0 0 0 1 0 0 0 (10H) Data (numeric)

1 0 0 0 1 0 1 1 (11H) &quot;

0 1 0 0 1 0 1 2 (12H) &quot;

1 1 0 0 1 0 0 3 (13H) &quot;

0 0 1 0 1 0 1 4 (14H) &quot;

1 0 1 0 1 0 0 5 (15H) &quot;

0 1 1 0 1 0 0 6 (16H) &quot;

1 1 1 0 1 0 1 7 (17H) &quot;

0 0 0 1 1 0 1 8 (18H) &quot;

1 0 0 1 1 0 0 9 (19H) &quot;

0 1 0 1 1 0 0 : (1AH) Special

1 1 0 1 1 0 1 ; (1BH) &quot;

0 0 1 1 1 0 0 &lt; (1CH) &quot;

1 0 1 1 1 0 1 = (1DH) &quot;

0 1 1 1 1 0 1 &gt; (1EH) &quot;

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) &quot;

1 1 0 0 0 1 0 C (23H) &quot;

0 0 1 0 0 1 1 D (24H) &quot;

1 0 1 0 0 1 0 E (25H) &quot;

0 1 1 0 0 1 0 F (26H) &quot;

1 1 1 0 0 1 1 G (27H) &quot;

0 0 0 1 0 1 1 H (28H) &quot;

1 0 0 1 0 1 0 I (29H) &quot;

0 1 0 1 0 1 0 J (2AH) &quot;

1 1 0 1 0 1 1 K (2BH) &quot;

0 0 1 1 0 1 0 L (2CH) &quot;

1 0 1 1 0 1 1 M (2DH) &quot;

0 1 1 1 0 1 1 N (2EH) &quot;

1 1 1 1 0 1 0 O (2FH) &quot;

0 0 0 0 1 1 1 P (30H) &quot;

1 0 0 0 1 1 0 Q (31H) &quot;

0 1 0 0 1 1 0 R (32H) &quot;

1 1 0 0 1 1 1 S (33H) &quot;

0 0 1 0 1 1 0 T (34H) &quot;

1 0 1 0 1 1 1 U (35H) &quot;

0 1 1 0 1 1 1 V (36H) &quot;

1 1 1 0 1 1 0 W (37H) &quot;

0 0 0 1 1 1 0 X (38H) &quot;

1 0 0 1 1 1 1 Y (39H) &quot;

0 1 0 1 1 1 1 Z (3AH) &quot;

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.

\*\* 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:

--------- &lt;edge of card&gt;

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

| ^ ^ ^

|------------------| 0.223&quot;--|---------|-------------------------

| | | 0.353&quot; | ^

|..................|.........|.........| 0.493&quot; |

| Track #1 0.110&quot; | | |

|............................|.........|... &lt;MAGSTRIPE&gt;

| | | |

|............................|.........|... |

| Track #2 0.110&quot; | |

|......................................|... |

| | |

|......................................|... |

| Track #3 0.110&quot; |

|.......................................... |

| |

|------------------------------------------------------------------

|

| &lt;body of card&gt;

|

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 &amp; Account

2 ABA 75 bpi BCD 40 Read Account

3 THRIFT 210 bpi BCD 107 Read Account &amp;

\*Encode\* Transaction

\*\*\* Track 1 Layout: \*\*\*

| SS | FC | PAN | Name | FS | Additional Data | ES | LRC |

SS=Start Sentinel &quot;%&quot;

FC=Format Code

PAN=Primary Acct. # (19 digits max)

FS=Field Separator &quot;^&quot;

Name=26 alphanumeric characters max.

Additional Data=Expiration Date, offset, encrypted PIN, etc.

ES=End Sentinel &quot;?&quot;

LRC=Longitudinal Redundancy Check

\*\*\* Track 2 Layout: \*\*\*

| SS | PAN | FS | Additional Data | ES | LRC |

SS=Start Sentinel &quot;;&quot;

PAN=Primary Acct. # (19 digits max)

FS=Field Separator &quot;=&quot;

Additional Data=Expiration Date, offset, encrypted PIN, etc.

ES=End Sentinel &quot;?&quot;

LRC=Longitudinal Redundancy Check

\*\*\* Track 3 Layout: \*\* Similar to tracks 1 and 2. Almost never used.

Many different data standards used.

Track 2, &quot;American Banking Association,&quot; (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 &quot;International Air Transport Association,&quot; 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 &quot;pops up&quot; 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:

&quot;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.&quot;

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.

\*\* A Bit About Magstripe Equipment \*\*

&quot;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!!&quot;

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 &quot;criminal motives.&quot; 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 &quot;swipe&quot; machines: the type you have to physically slide the card thru.

Others are &quot;insertion&quot; 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. &quot;Hey son, what are you doing with our model XYZ swipe reader?

That belongs in the hands of a &quot;qualified&quot; merchant or retailer, not some punk

kid trying to &quot;find out how things work!&quot; 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!).

\*\* 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 &quot;common data.&quot; 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 &quot;x&quot;'s.

In those cases, NUMBER of CHARACTERS was consistent (the number of &quot;x&quot;'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! &quot;Hey, can I, ahh, like BORROW your MCI calling card tonight? I'm

working on an, ahh, EXPERIMENT. Please?&quot; 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!

-------------------------------------------------------------------------------

-=Mastercard=- Number on front of card -&gt; 1111 2222 3333 4444

Expiration date -&gt; 12/99

Track 2 (BCD,75 bpi)-&gt; ;1111222233334444=99121010000000000000?

\*\*\*

Track 1 (ALPHA,210 bpi)-&gt; %B1111222233334444^PUBLIC/JOHN?

\*

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

-------------------------------------------------------------------------------

-=VISA=- Number on front of card -&gt; 1111 2222 3333 4444

Expiration date -&gt; 12/99

Track 2 (BCD,75 bpi)-&gt; ;1111222233334444=9912101xxxxxxxxxxxxx?

\*\*\*

Track 1 (ALPHA,210 bpi)-&gt; %B1111222233334444^PUBLIC/JOHN^9912101xxxxxxxxxxxxx?

\*

Note that the &quot;101&quot; was common to all VISA cards checked, as well as the &quot;B&quot;.

Also, the &quot;xxx&quot; 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.

-------------------------------------------------------------------------------

-=Discover=- Number on front of card -&gt; 1111 2222 3333 4444

Expiration date -&gt; 12/99

Track 2 (BCD,75 bpi)-&gt; ;1111222233334444=991210100000?

\*\*\*\*\*\*\*\*

Track 1 (ALPHA,210 bpi)-&gt; %B1111222233334444^PUBLIC/JOHN\_\_\_^991210100000?

\*\*\*\*\*\*\*\*

Note, the &quot;10100000&quot; and &quot;B&quot; were common to most DISCOVER cards checked. I

found a few that had &quot;10110000&quot; 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

&quot;padded&quot; with SPACES. So...for all of you with names longer than 25 (exclude

the &quot;/&quot;) characters, PREPARE to be TRUNCATED! ;)

-------------------------------------------------------------------------------

-=US Sprint FON=- Number on front of card -&gt; 111 222 3333 4444

Track 2 (BCD,75 bpi)-&gt; ;xxxxxx11122233339==xxx4444xxxxxxxxxx=?

\*

Track 1 (ALPHA,210 bpi)-&gt; %B^ /^^xxxxxxxxxxxxxxxxx?

\*

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 &quot;xxx&quot;

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.

-------------------------------------------------------------------------------

-=Fleet Bank=- Number on front of card -&gt; 111111 222 3333333

Expiration date -&gt; 12/99

Track 2 (BCD,75 bpi)-&gt; ;1111112223333333=9912120100000000xxxx?

\*\*\*\*

Track 1 (ALPHA,210 bpi) -&gt;

%B1111112223333333^PUBLIC/JOHN\_\_\_^9912120100000000000000xxxx000000?

\* \*\*\*\*

Note that the &quot;xxx&quot; data varied. This is the encrypted PIN offset. Always 4

digits (hmmm...). The &quot;1201&quot; was always the same. In fact, I tried many ATM

cards from DIFFERENT BANKS...and they all had &quot;1201&quot;.

-------------------------------------------------------------------------------

(Can't leave \*this\* one out ;)

-=Radio Shack=- Number on front of card -&gt; 1111 222 333333

NO EXPIRATION data on card

Track 2 (BCD,75 dpi)-&gt; ;1111222333333=9912101?

\*\*\*\*\*\*\*

Note that the &quot;9912101&quot; 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.

\*\* 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

&quot;shadow pattern&quot; 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&quot;). These cards are quite thick, up to

0.15&quot; (the ABA standard is 0.030&quot;!).

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 &quot;spots&quot; 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.

\*\* 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.

\*\* 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.

\*\* 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.

\*\* 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 &quot;corporate conspiracy,&quot; 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. &quot;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?&quot; heh heh

\*\* 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

&quot;Restricted Data Transmissions&quot;...a group of techies based in the Boston area

that feel that &quot;Information is Power&quot;...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.... &quot;Truth is cheap, but information costs!&quot;

But -=RDT is gonna change all that... ;) set the info FREE!

Peace.

..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 &quot;ATDT&quot;...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.. ;)

</pre>

</div>

</div>

</center>

<div align="center" class="texto-2-bold">

[ <a href="../../index.html" title="News">News</a> ]

[ <a href="../../papers/shockwave\_memory\_disclosure.html" title="Paper Feed">Paper Feed</a> ]

[ <a href="../../issues/68/1.html" title="Issues">Issues</a> ]

[ <a href="../../authors.html" title="Authors">Authors</a> ]

[ <a href="../../archives/" title="Archives">Archives</a> ]

[ <a href="../../contact.html" title="Contact">Contact</a> ]

</div>

<div align="right" class="texto-1">© Copyleft 1985-2014, Phrack Magazine.</div>

</body>

</html>