Privacy Implications of Magstripes

Acidus (acidus@msblabs.org)
Most Significant Bit Labs
http://www.msblabs.org

Toorcon 6 – Sept 26, 2004

Overview

- Magstripes? Why?
- Basics of magstripe cards
- Privacy issues and concerns
- What can we do about it?
- What's the future of physical authentication?

History

- Why write about magstripes?
  - *Card-o-ramra*, Count Zero, Phrack 37, 1992
  - *Interfacing a TTL magcard*... Patrick Gueull, PDF, 1997
  - Some text files, academic papers
  - Kind of a lost art. The people that need to know already know. Small enough industry that it stays that way

Magstripe Basics

- Plastic, magnets, and glue
- 3 tracks
  - Track 1 – Alpha-numeric (IATA)
  - Track 2 – Numeric, most common (ABA)
  - Track 3 – anything goes! read.write (old ATM days)
- Analog – uses magnetic fluxes

Magstripe Basics

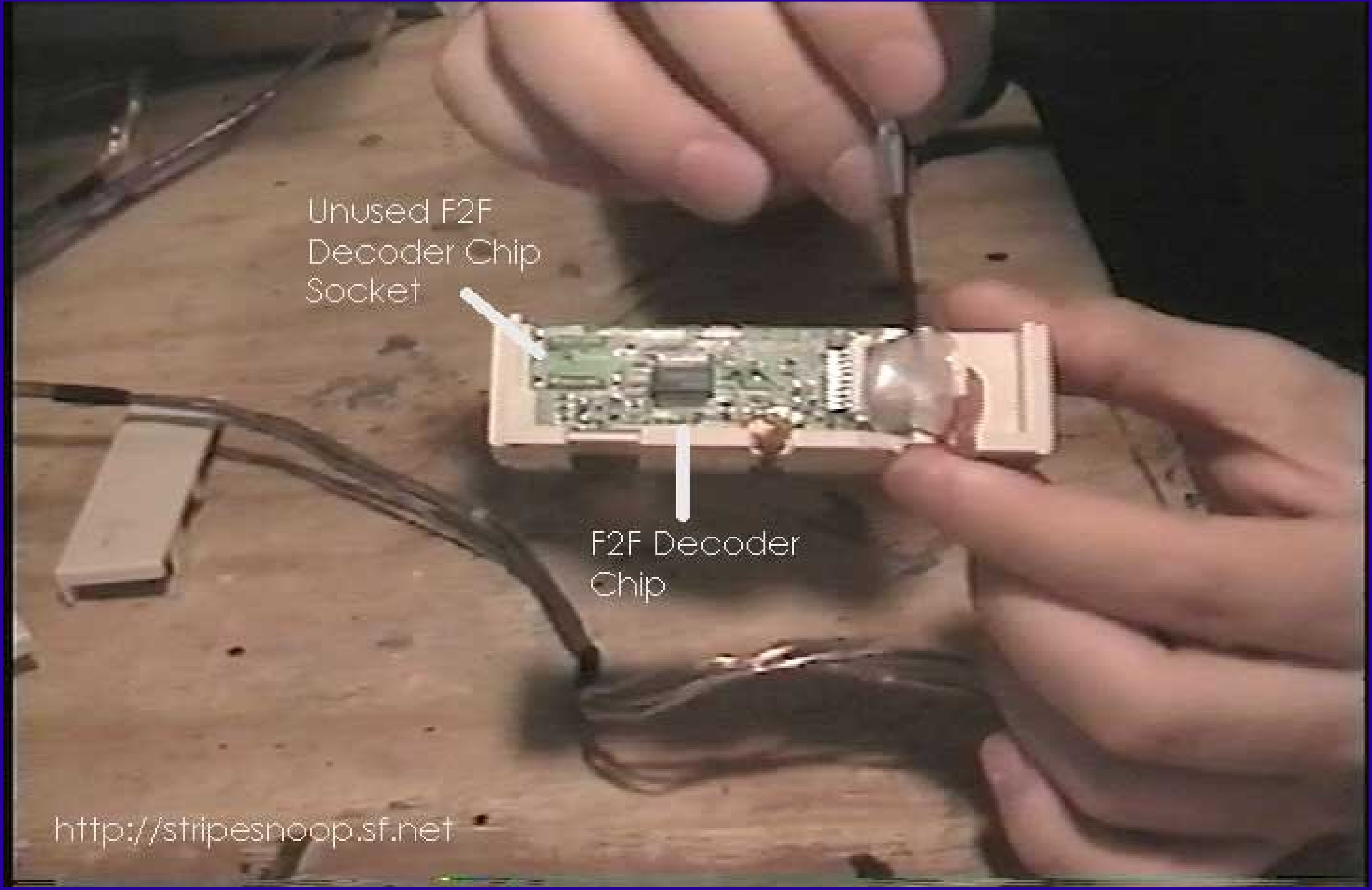
- F2F Chips (Flux to Flux decoder)
  - There things rule! (Magtek)
  - Basically an ADC
  - Analog magnetic fluxes go in, bitstream of card data comes out
  - Has no concept of a “track” or bit density
  - Supports all 3 tracks

TTL Readers

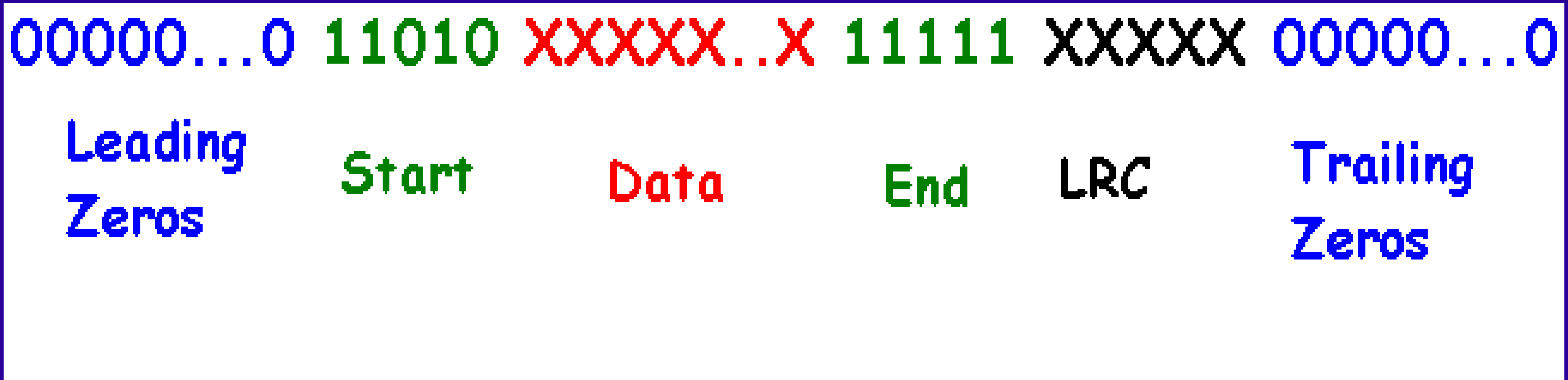
- Makes interfacing easy
- Uses F2F chips
- Cheap! (~$15 @ Digikey, $3 @ BGMicro)
- Take in 5V and ground
- Card Present, Data/Clock pairs per track
- Produces a bitstream for each track

What does it look like?

TTL Readers


Unused F2F
Decoder Chip
Socket
F2F Decoder
Chip
http://stripesnoop.sf.net

Magstripe Bitstream

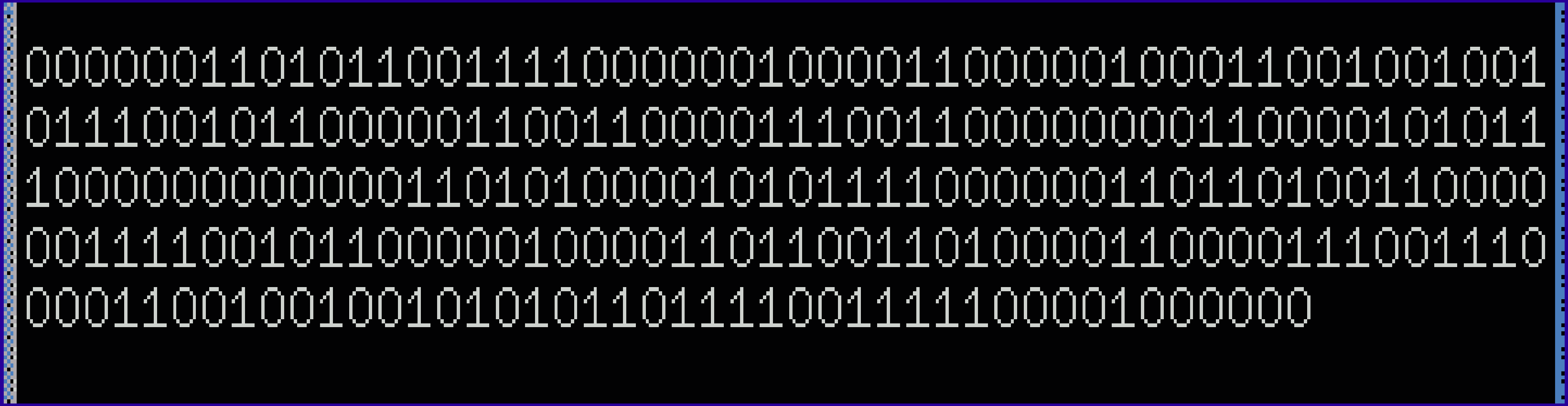


00000...0	11010	XXXXX..X	11111	XXXXX	00000...0
Leading Zeros	Start	Data	End	LRC	Trailing Zeros

Magstripe Bitstream

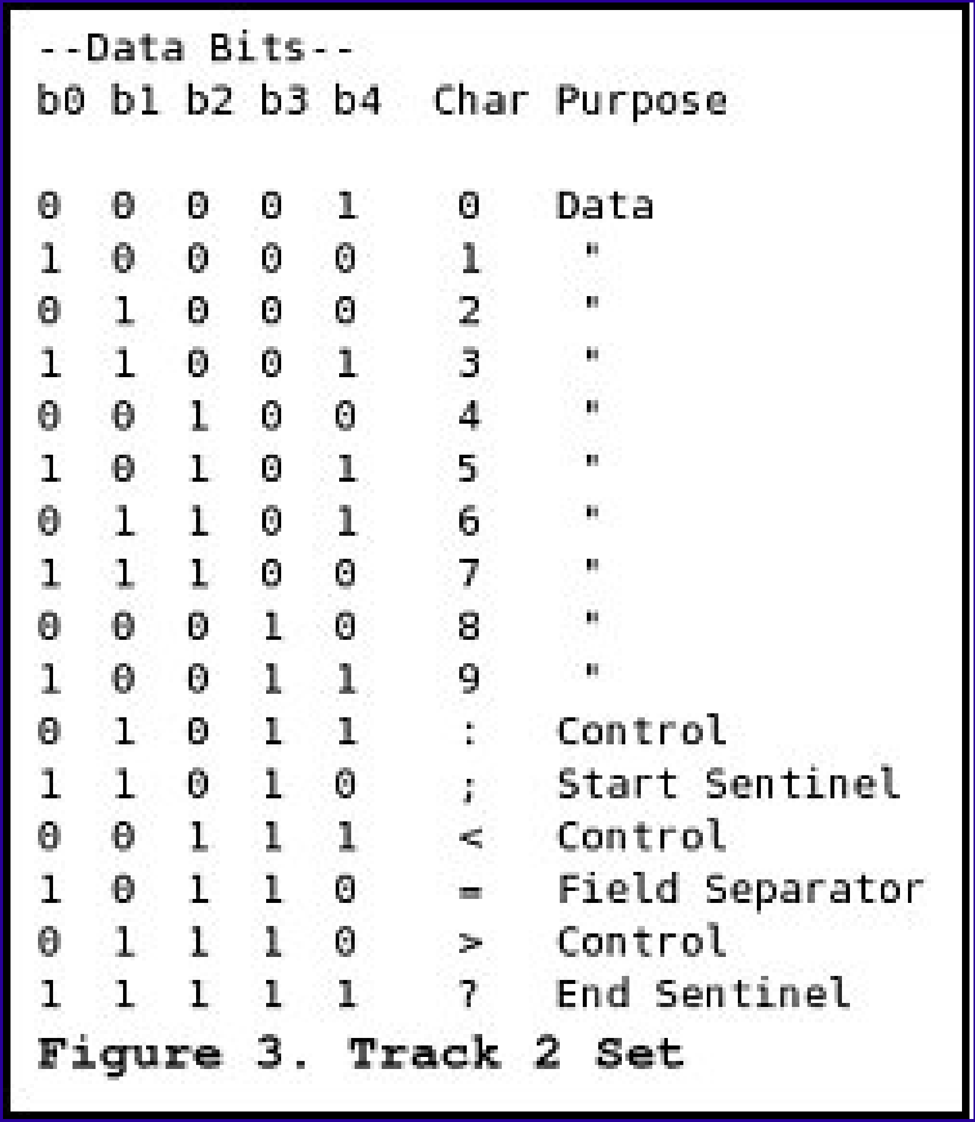
- Leading zeros are for syncing
- Trailing zeros are for backward swipes
- LRC is to make it all OK
- Character set varies
  - Track 1 – 64 characters (lower ASCII) 6 data + 1 parity
  - Track 2 – 16 charters (0-9, control) 4 data + 1 parity

Example Bitstream



```
0000001101011001111000000100001100000100011001001001
0111001011000001100110000111001100000000110000101011
1000000000000110101000010101111000000110110100110000
0011110010110000010000110110011010000110000111001110
00011001001001010101101111001111100001000000
```

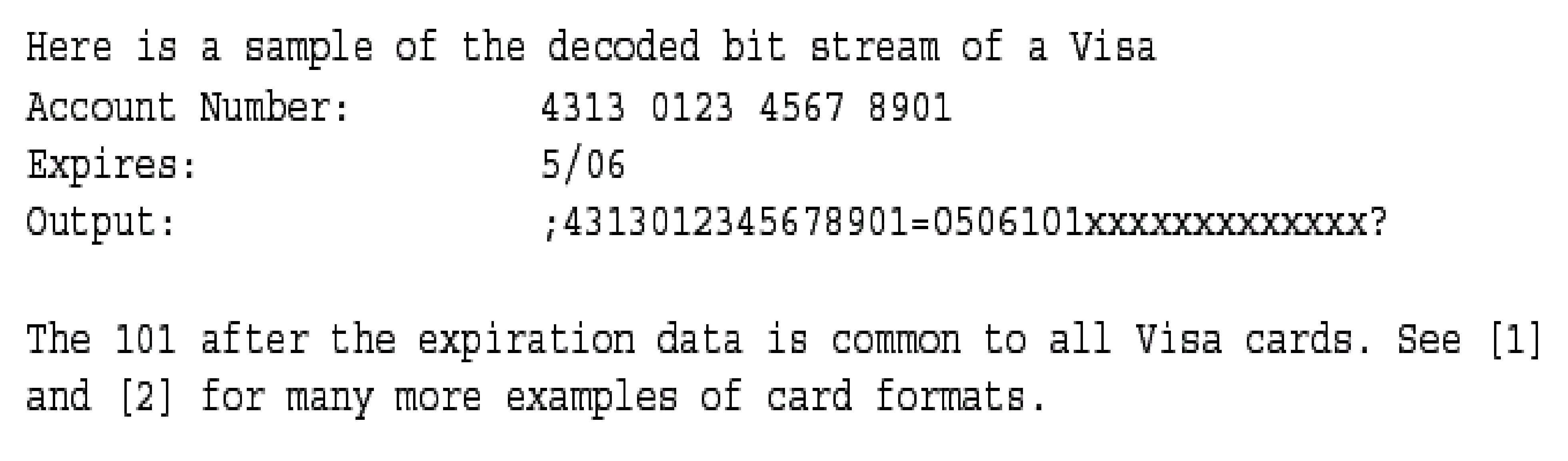
ABA Track 2 Character Set



--Data Bits--						
b0	b1	b2	b3	b4	Char	Purpose
0	0	0	0	1	0	Data
1	0	0	0	0	1	"
0	1	0	0	0	2	"
1	1	0	0	1	3	"
0	0	1	0	0	4	"
1	0	1	0	1	5	"
0	1	1	0	1	6	"
1	1	1	0	0	7	"
0	0	0	1	0	8	"
1	0	0	1	1	9	"
0	1	0	1	1	:	Control
1	1	0	1	0	;	Start Sentinel
0	0	1	1	1	<	Control
1	0	1	1	0	=	Field Separator
0	1	1	1	0	>	Control
1	1	1	1	1	?	End Sentinel

Figure 3. Track 2 Set

Card Sample



```
Here is a sample of the decoded bit stream of a Visa
Account Number:        4313 0123 4567 8901
Expires:               5/06
Output:                ;4313012345678901=0506101xxxxxxxxxxxxx?
```

The 101 after the expiration data is common to all Visa cards. See [1] and [2] for many more examples of card formats.

So What?

- Come on Acidus!
- All this stuff is already on the card!
- Where are the privacy concerns?

Its all about speed!

In 5 Seconds I Can Harvest...

- Social Security Numbers (and state of birth, approx year of issue)
- Date of birth
- Full address
- Telephone number
- Medical info (glasses/contacts, blood type, height, weight)

Worst Offenders

- Student IDs (thanks GaTech, Blackboard)
- Insurance cards (SSN)
- Driver's licenses (Contact info, medical conditions)
- Membership cards (and their not so random unique ID numbers)

How We Protect Ourselves?

- Audit your cards. Find out what's on them
- Talk with the companies. See if they are lying
- Do you need it?
- Erasing private info (spot erasing, total)

How Can We Have Some Fun?

- Companies paid for all this infrastructure
- Build fun applications on top of everything!
- Void some warranties
- Make large DC based companies hate you
- Show people how silly it all is

Something I'm gagged for 2 years from doing: Creating and sharing a better solution

Putting It All Together

- Maghead reads fluxes from cards
- F2F chip converts card data into bitstream
- ISO standards tell us format of the data
- All we need is a computer interface
  - Gameport
  - Parallel Port
  - USB (Cypress chipsets are cheap)

Gameport Interface

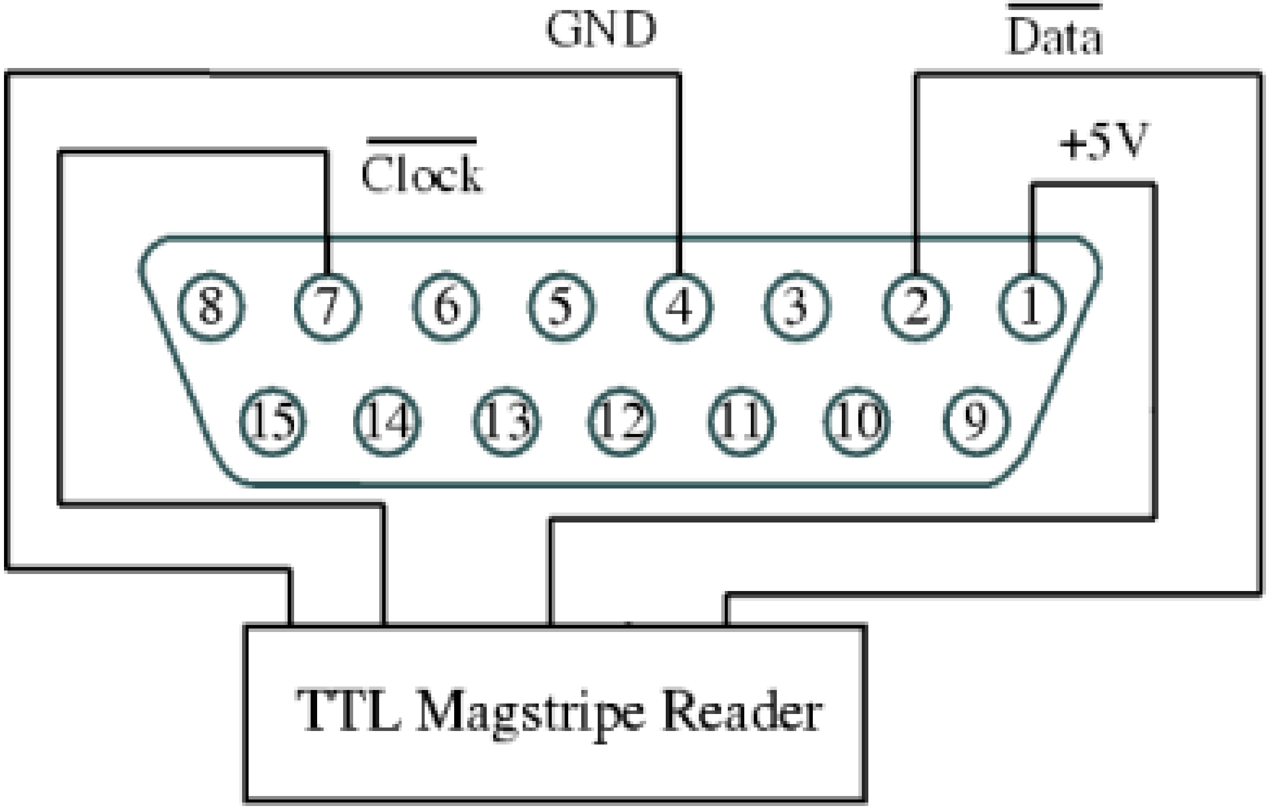
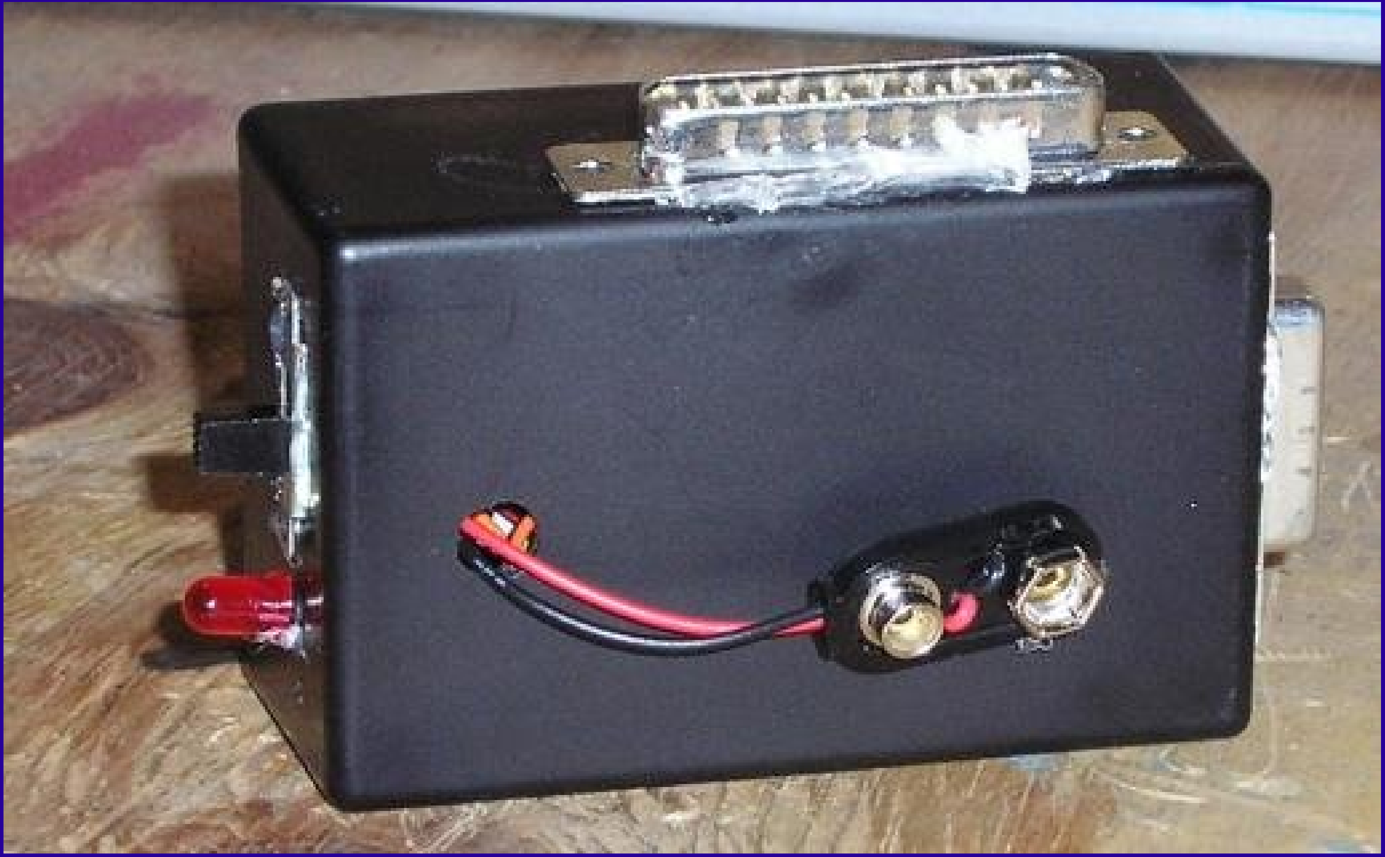


Figure 1. Wiring the Magstripe

Parallel Port Interface



Sample Applications

- Card research (Stripe Snoop)
- Unix/Linux PAM modules
- Coke Machine (and more...)
- Internet gift card sharing?
- Lays framework, methodology for tools for new techs (RFID, smart cards)

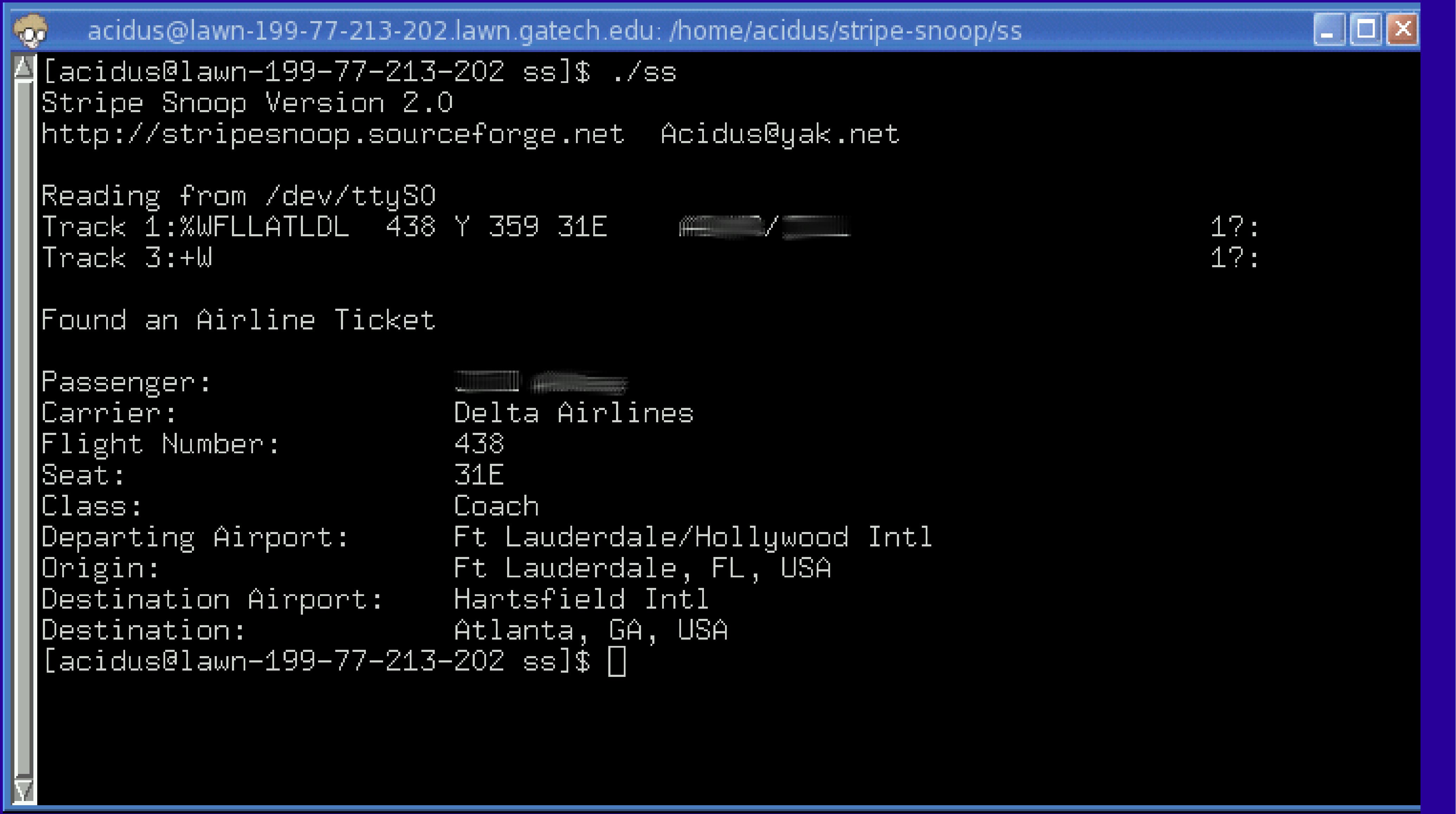
Stripe Snoop

http://stripesnoop.sourceforge.net

Stripe Snoop

- Reads bitstream from various hardware interfaces
- Decodes to appropriate character set
- Looks up card fingerprint in database to decode card's data fields
- Released under GPL
- Windows, Linux, Mac

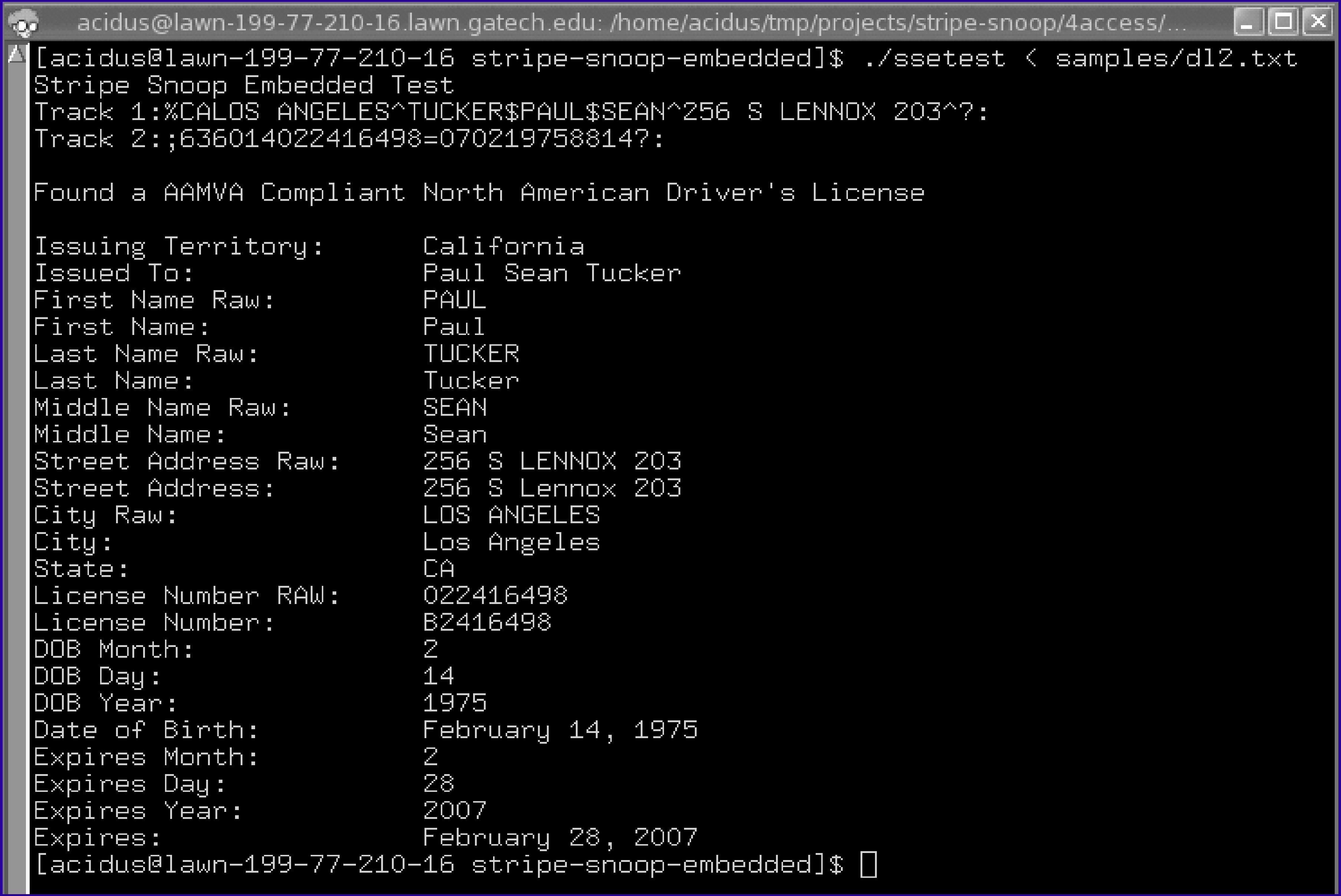
Stripe Snoop: Plane Ticket



acidus@lawn-199-77-213-202.lawn.gatech.edu: /home/acidus/stripe-snoop/ss

```
[acidus@lawn-199-77-213-202 ss]$ ./ss
Stripe Snoop Version 2.0
http://stripesnoop.sourceforge.net  Acidus@yak.net

Reading from /dev/ttyS0
Track 1:%WFLLATLDL  438 Y 359 31E    [redacted]/[redacted]                    1?:
Track 3:+W                                                                    1?:

Found an Airline Ticket

Passenger:                [redacted]
Carrier:                  Delta Airlines
Flight Number:            438
Seat:                     31E
Class:                    Coach
Departing Airport:        Ft Lauderdale/Hollywood Intl
Origin:                   Ft Lauderdale, FL, USA
Destination Airport:      Hartsfield Intl
Destination:              Atlanta, GA, USA
[acidus@lawn-199-77-213-202 ss]$ □
```

Stripe Snoop: Driver's License


acidus@lawn-199-77-210-16.lawn.gatech.edu: /home/acidus/tmp/projects/stripe-snoop/4access/...

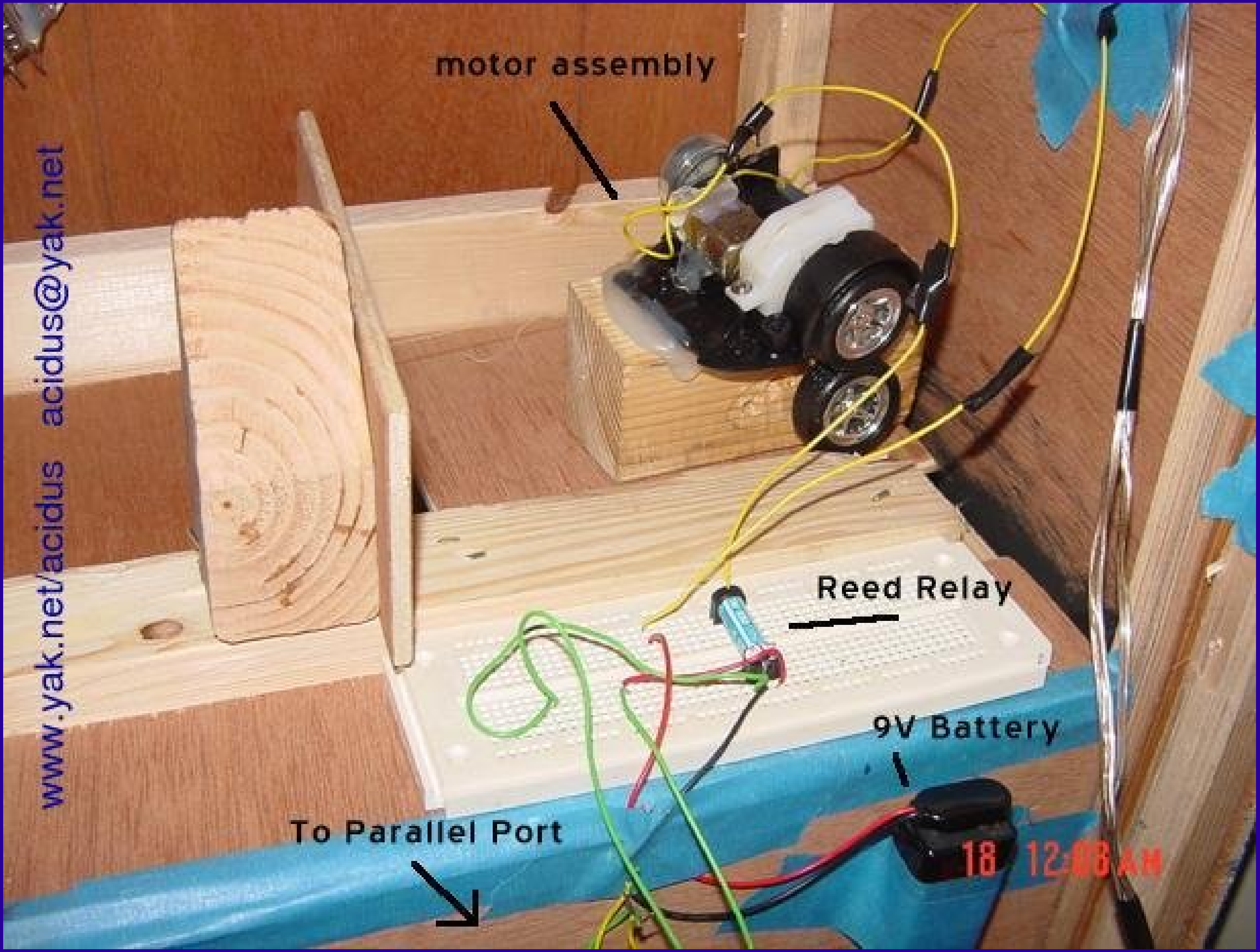
```
[acidus@lawn-199-77-210-16 stripe-snoop-embedded]$ ./ssetest < samples/dl2.txt
Stripe Snoop Embedded Test
Track 1:%CALOS ANGELES^TUCKER$PAUL$SEAN^256 S LENNOX 203^?:
Track 2:;636014022416498=070219758814?:

Found a AAMVA Compliant North American Driver's License

Issuing Territory:      California
Issued To:              Paul Sean Tucker
First Name Raw:         PAUL
First Name:             Paul
Last Name Raw:          TUCKER
Last Name:              Tucker
Middle Name Raw:        SEAN
Middle Name:            Sean
Street Address Raw:     256 S LENNOX 203
Street Address:         256 S Lennox 203
City Raw:               LOS ANGELES
City:                   Los Angeles
State:                  CA
License Number RAW:     022416498
License Number:         B2416498
DOB Month:              2
DOB Day:                14
DOB Year:               1975
Date of Birth:          February 14, 1975
Expires Month:          2
Expires Day:            28
Expires Year:           2007
Expires:                February 28, 2007
[acidus@lawn-199-77-210-16 stripe-snoop-embedded]$
```

Coke Machine

Coke Machine

- Computer controls it all
  - Reads TTL reader through gameport
  - Controls motors of Coke machine with relays through parallel port
- Rather overpowered. Could have used microcontroller instead

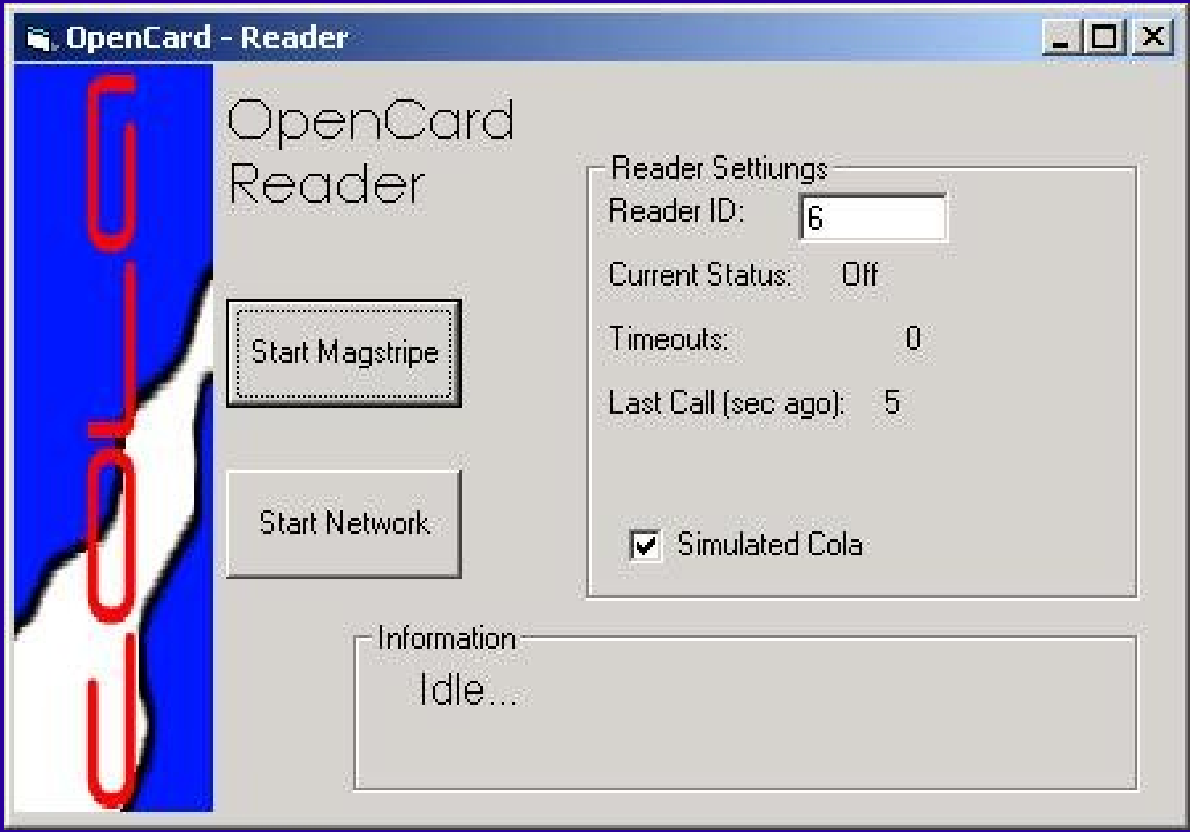
Coke Machine



Could We Go Further...

and make a full transaction system that doesn't suck?

Maybe I already did and just can't tell you...



OpenCard - Reader

OpenCard Reader

Reader Settiungs

Reader ID: 6

Current Status: Off

Timeouts: 0

Last Call (sec ago): 5

☑ Simulated Cola

Information

Idle...

Future of Physical Authentication?

- Smart cards
- RFID
- Bluetooth
- “The Handshake”

Smart cards

- 1st generation (stored value, memory in a card, AMEX Blue)
- 2nd generation (PKI, protect contents)
- All over Europe (leaped a tech like China and cellphones)
- Digit cash scare in mid 90s
- Never going to be big in US

RFID: The Big Scary

- Extension of prox cards (13.5 Mhz)
- Brew of standards
- RFDump, the Ethereal of RFID
- California law re: destruction, too much?
- I'm all for RFID! Companies spend millions deploying infrastructure, we create applications that run on top of it!

Bluetooth

- Japan loves this. Cellphone is your life
- Pretty good architecture
  - Stack can run other protocols
  - Reasonably mature
- Hacks
  - Remote reading (almost cancer free!)
  - Forced re-peering, compromises keys

The Handshake

- IBM has a patent on this
- Part of a Personal Area Network (PAN)
- Embedded chip in body, clothes
- Physical touch does a 1 wire protocol like an iButton
- Shake hands, exchange business cards
- Judge Dredd: gun only works with cops

Future

- Build a magstripe reader, check what you have
- Blank what you can
- Spread awareness
- Pay addition to new technologies, standards. Committees are frequently stupid (WEP anyone?)

Questions?

Privacy Implications of Magstripes

Acidus (acidus@msblabs.org)
Most Significant Bit Labs
http://www.msblabs.org

Toorcon 6 – Sept 26, 2004