



Notacon Mythbusters: Is Personal Data Stored on Hotel Keys?

Using Magstripe Analysis Tools to Discover the Answer

By: Matt “Zamboni” Neely

Presented: April 17, 2009 at Notacon 6



- Matt “Zamboni” Neely - Manager of the Profiling team at SecureState:
 - Areas of expertise include: wireless security, penetration testing, physical security, security convergence and incident response
 - 10 years of security experience
 - Presented at DEFCON 13 and ShmooCon 2009
- Outside of work:
 - Co-host of the Security Justice Podcast
 - Board member for the North Eastern Ohio Information Security Forum



Southern California law enforcement professionals assigned to detect new threats to personal security issues recently discovered what type of information is embedded in the credit card type hotel room keys used through-out the industry.

Although room keys differ from hotel to hotel, a key obtained from the Double Tree chain that was being used for a regional Identity Theft Presentation was found to contain the following information:

- Customer's (your) name
- Customer's partial home address
- Hotel room number

Truth or Fiction?

Check in date and check out date
Customer's (your) record card number and expiration date!
When you turn them in to the front desk your personal information is there for any employee to access by simply scanning the card in the hotel scanner. An employee can take a hand full of cards home and, using a scanning device, access the information onto a laptop computer and go shopping at your expense.

Simply put, hotels do not erase these cards until an employee issues the card to the next hotel guest. It is usually kept in a drawer at the front desk with **YOUR INFORMATION ON IT!!!!**

The bottom line is, keep the cards or destroy them! NEVER leave them behind and NEVER turn them in to the front desk when you check out of a room. They will not charge you for the card.

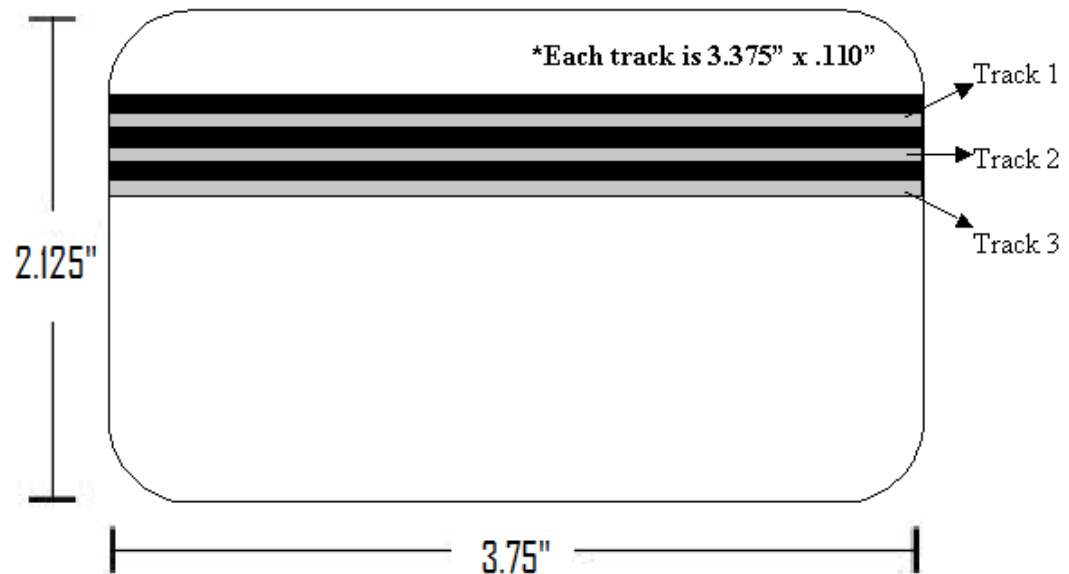


- Brief introduction to magnetic stripe (magstripe) cards
- Overview of tools to read magstripe cards
- Test the Myth
- View the results
- Advanced magstripe analysis



What Are Those Magical Stripes?

- ISO 7810 – Physical characteristics of the card
- ISO 7811 – How data is recorded
 - Three tracks (ISO-1, ISO-2, ISO-3)
 - Coercivity (HiCo vs. LoCo)
- ISO 7813 – Format of encoded data on financial transaction cards





- Track 1

- IATA – 210 BPI, 7 bit (including parity bit), 79 alphanumeric characters and special characters ^ % ?

| | | | | | | | |
|---|-------------------|---|-------------------|---|-------------------|---|-----|
| % | Alphanumeric Data | ^ | Alphanumeric Data | ^ | Alphanumeric Data | ? | LRC |
|---|-------------------|---|-------------------|---|-------------------|---|-----|

- Track 2

- ABA – 75 BPI, 5 bit (including parity bit), 40 numeric character and special characters : ; < = > ?

| | | | | | | | |
|---|--------------|---|--------------|---|--------------|---|-----|
| : | Numeric Data | = | Numeric Data | = | Numeric Data | ? | LRC |
|---|--------------|---|--------------|---|--------------|---|-----|

- Track 3

- THIFT – 210 BPI, 5 bit (including parity bit), 107 numeric characters and special characters : ; < = > ?

| | | | | | | | |
|---|--------------|---|--------------|---|--------------|---|-----|
| : | Numeric Data | = | Numeric Data | = | Numeric Data | ? | LRC |
|---|--------------|---|--------------|---|--------------|---|-----|



- <http://stripesnoop.sourceforge.net/>
- Free
- Open source
- Supports Windows 9x, NT, 2K, XP and Linux
- Limited ability to parse non-standard formats
- Automatically identifies certain cards
- Reader options
 - Build your own
 - POS keyboard readers



- <http://www.makinterface.de/makstusbe.php3>
- Commercial
 - USB reader/writer for 199 EUR (298.50 USD)
- Older versions used a parallel port reader/writer
- Supports Windows NT/2000/XP/Vista, Linux, Mac OS and WM5/6
- Reads all three tracks
- Supports standard and non-standard formats
- Advanced analysis and data visualization tools
- Card writer
 - Special features that assist in manipulating cards
 - Automatically calculate checksums after manipulating data
- The best reader for looking at non-standard magstripe cards



Character Decode

Decode **Char**

Signal Analysis

Data Analysis

Write Track

Track#1 **189 BPI** %B3702 650191 93060^ / ^170410107022381101?H

| | | | |
|----------|-------------|--------------------|---------------------------|
| Char set | ALFA | B3702 650191 93060 | Start Sentinel : % |
| Chars | 67 | / | Data : B3702 650191 93060 |
| Parrrity | Ok | 170410107022381101 | Field Separator: ^ |
| LRC | Ok | | Data : / |
| | | | Field Separator: ^ |

Track#2 **70 BPI** ;370265019193060=170410107022381101000?6

| | | | |
|----------|------------|-----------------------|------------------------------|
| Char set | BCD | 370265019193060 | Start Sentinel : ; |
| Chars | 40 | 170410107022381101000 | Data : 370265019193060 |
| Parrrity | Ok | | Field Separator: = |
| LRC | Ok | | Data : 170410107022381101000 |
| | | | End Sentinel : ? |

Track#3

| | | | |
|----------|--|--|--|
| Char set | | | |
| Chars | | | |
| Parrrity | | | |
| LRC | | | |



ISO Decode

Decode **ISO**

Signal Analysis

Data Analysis

Write Track

Track#1 **189 BPI** %B3702 650191 93060^ / ^170410107022381101?H

| | | | |
|-----------------|-------------|--|---|
| Char set | ALFA | Start Sentinel : % | ↑ |
| Chars | 67 | Format Code : B | ⋮ |
| Parrrity | Ok | Primary Account Nummber : 3702 650191 93060 [Card nummber (Luhns Algorithmus)is INVALID] | ↓ |
| LRC | Ok | Field Separator : ^ | |
| | | Name : / | |

Track#2 **70 BPI** ;370265019193060=170410107022381101000?6

| | | | |
|-----------------|------------|---|---|
| Char set | BCD | Start Sentinel : ; | ↑ |
| Chars | 40 | Primary Account Nummber : 370265019193060 | ⋮ |
| Parrrity | Ok | Field Separator : = | ↓ |
| LRC | Ok | Expiration date : 04/17 | |
| | | Service code : 101 | |

Track#3

| | | | |
|-----------------|--|--|---|
| Char set | | | ↑ |
| Chars | | | ⋮ |
| Parrrity | | | ↓ |
| LRC | | | |



Magnetic-Stripe Card Explorer

File Setup About

Scan Port for Data **Autoexit**
 Error correction
Stop Scanning

Status: Idle

Decode | **Signal Analysis** | **Data Analysis** | **Write Track**

Source data
 Track#1
 Track#2
 Track#3
 Custom

Destination
 Track#1
 Track#2
 Track#3

Reference Track
 Track#1
 Track#2
 Track#3

Prepare to write
Erase #1 **eBASE**
Format Reference Track #2
Duration seconds

Write data to Track
0/1 adj.
BPI adj.
Write Track
 Swipe speed=Ref.

Custom data

Data

Auto properties
Load
Save

Copy from Track
Copy
 Track#1
 Track#2
 Track#3

Insert special chars
Start Sentinel
Field Separator
End Sentinel
Insert LRC

Data properties
Nr. of Chars Total nr. of Bits
Character set Bits before data
BitsPerInch Bits in data
 recalculate LRC Bits after data



TEST THE MYTH



- Gathered approximately 25 magstripe hotel key from a variety of hotels
- Group cards by hotel and room number
- Read each card multiple times and compared the output to ensure data was correctly read from the cards
- Analyzed the result...



- Every hotel card had data on track 3, some had data on additional tracks
- Same data was encoded between multiple tracks
- Standard ALFA or BCD character sets were not used
- Tried various groupings but could not generate a valid checksum or parity bits
- Often times the data varied greatly between two cards for the same room
- One exception was that the data between two cards for the same room were off by 28 bits



Observe the Process

- Talked with a number of hotel employees at different hotels
- Older card encoders are stand alone devices that only require the room number and check-out date to encode a card
- Newer systems connect into the front desk registration PC and require no user input



The screenshot shows a Mozilla Firefox browser window with the address bar containing `http://www.snopes.com/crime/warnings/hotelkey.asp`. The page title is "snopes.com: Hotel Key Card Identity Theft - Mozilla Firefox". The browser's menu bar includes File, Edit, View, History, Bookmarks, Tools, and Help. The address bar has navigation buttons (back, forward, home, search) and a search engine dropdown set to Google. Below the address bar is a toolbar with various utility icons like Disable, Cookies, CSS, Forms, Images, Information, Miscellaneous, Outline, Resize, Tools, and View.

The main content of the page is as follows:

[Home](#) --> [Crime](#) --> [Warnings](#) --> [Card Sharks](#)

Card Sharks

Claim: Hotel room keycards are routinely encoded with personal information which can be easily harvested by thieves.

Status: *False.*

Examples:

[Collected on the Internet, 2003]

Southern California law enforcement professionals assigned to detect new threats to personal security issues, recently discovered what type of information is embedded in the credit card type hotel room keys used through-out the industry.

Although room keys differ from hotel to hotel, a key obtained from the Double Tree chain that was being used for a regional Identity Theft

The browser's status bar at the bottom shows "Done", "Proxy: None", the IP address "66.165.133.65", and the server type "Microsoft-IIS/5.0". There are also icons for JavaScript and SSL.



BUSTED



ADVANCED MAGSTRIPE ANALYSIS



Signal Analysis

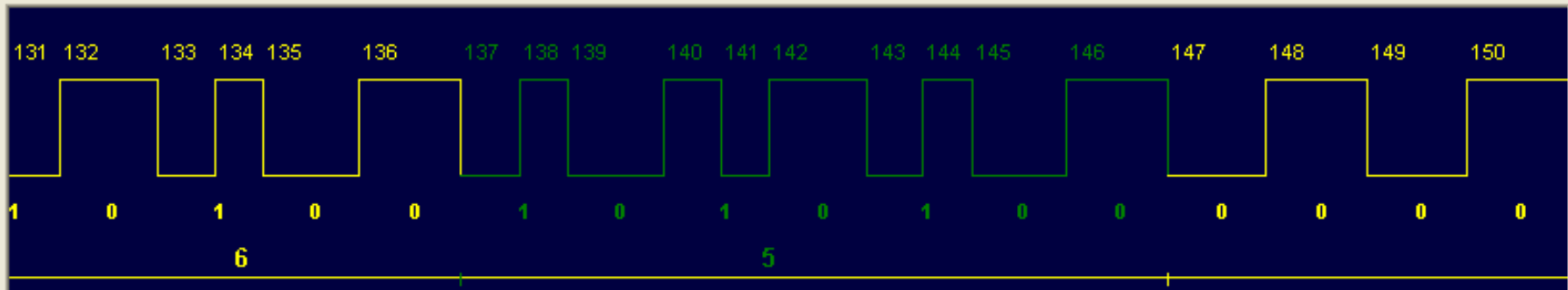
Decode

Signal Analysis

Data Analysis

Write Track

Position < _____ > Zoom _____



Select Track

- Track#1
- Track#2
- Track#3

Display options

Auto - Zoom

Track density (BPI)

189

Total number of Ticks

777

First "1" Bit found at position

59

Character Set found

ALFA

| Tick | Char | Nr. | Flux | us | Bit |
|------|------|-----|------|-----|-----|
| 137 | 5 | 9 | 0 | 248 | 0.5 |
| 138 | 5 | 9 | 1 | 212 | 0.5 |
| 139 | 5 | 9 | 0 | 412 | 0 |
| 140 | 5 | 9 | 1 | 242 | 0.5 |
| 141 | 5 | 9 | 0 | 212 | 0.5 |
| 142 | 5 | 9 | 1 | 418 | 0 |
| 143 | 5 | 9 | 0 | 236 | 0.5 |
| 144 | 5 | 9 | 1 | 212 | 0.5 |
| 145 | 5 | 9 | 0 | 406 | 0 |
| 146 | 5 | 9 | 1 | 436 | 0 |
| 147 | 0 | 10 | 0 | 424 | 0 |
| 148 | 0 | 10 | 1 | 436 | 0 |
| 149 | 0 | 10 | 0 | 424 | 0 |

Delete Character 5

Ticks 137 - 146

Delete

Modify Character 5

Insert Character(s) after Tick 146

Work on

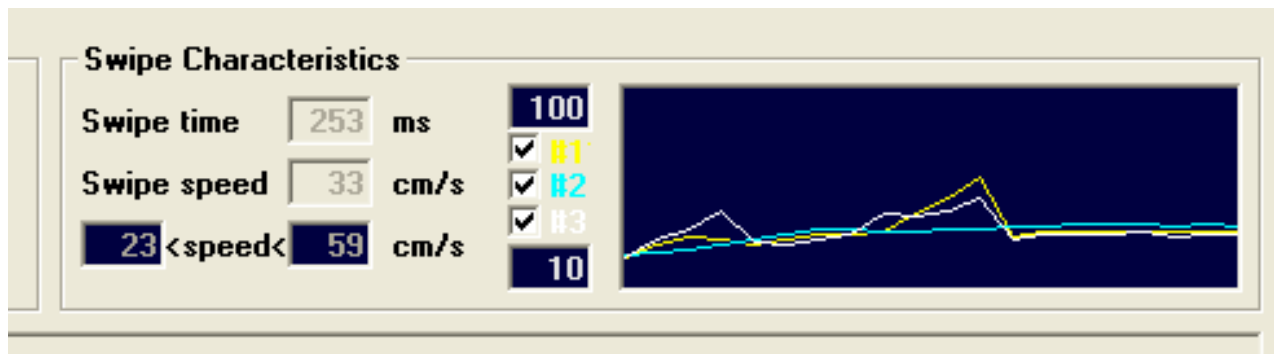
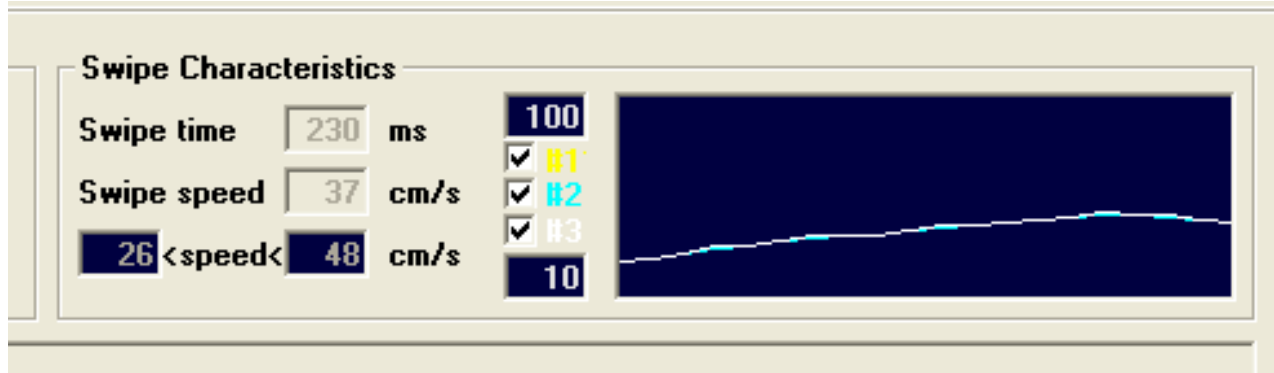
Ticks

Characters

AutoRecalc LRC



Tracks Written At Different Times





MAGNETIC DEVELOPER



Magnetic Developer

- Displays the magnetic pattern on a magstripe
- Q-View by Q-Card
 - www.q-card.com
 - \$44 a bottle (2 Oz.)
 - Spray or eye dropper application
- Will not damage the card
 - Developer can be wiped off after use
 - Cover magstripe with clear tape if you need to preserve the pattern





INSERT OR SWIPE KEY
 INSERITE O BARRIE LA LLAVE
 INSERREZ OU PATES GLISSER
 LA CLE DANS LA FENTE
 SCHLÜSSEL, ENGSTECKEN
 ODER DURCHGLEITEN
 5-1-8-8-37-2562
 1-877-837-2562
 免費熱線 800-837-2562



REMOVE KEY
 RETIREZ LA LLAVE
 RETIREZ LA CLE
 SCHLÜSSEL, ENTFERNEN
 5-1-8-8-37-2562
 1-877-837-2562
 免費熱線 800-837-2562

TURN HANDLE
 TOURNER LA POIGNÉE
 押下レバーを押す
 操作手順

www.dnity.com

CARIBOU COFFEE

Welcome to the CariBREW Club®.

When you present this card with payment at participating Caribou Coffee locations, you will earn rewards based on dollars spent. This CariBREW Club card must be registered to redeem rewards. To register this card or check point balances, go to www.cariboucoffee.com/cariBREWclub.

Use of this card constitutes acceptance of all program terms. Complete program details are available at www.cariboucoffee.com/cariBREWclub. This card is not redeemable for cash.

© 2007 Caribou Coffee Company, Inc.



FOR YOUR SECURITY

- Use safe deposit box for valuables.
- Secure desktop and downspout.
- Use viewport to ID all visitors.
- Employees are required to wear name tags.
- Sequester and keep your keypad with you at all times.
- Ensure that all windows and doors are locked.

PU

Operator Instructions

Insert
 Insert Card into Slot

Remove
 Remove Card from Slot

Open
 When Green Light Appears,
 Depress Lever and Open Door

To reorder, call:
 1-877-837-2562.

Dnity

© 2007-08 Dnity





Access Control System Attacks

- Example access card format for a centrally managed system

| | | | | | |
|---|-----------|---|--------------|---|-----|
| % | Site Code | ^ | Badge Number | ? | LRC |
|---|-----------|---|--------------|---|-----|

- Fuzz badge number

- Example access card format for a stand alone system:

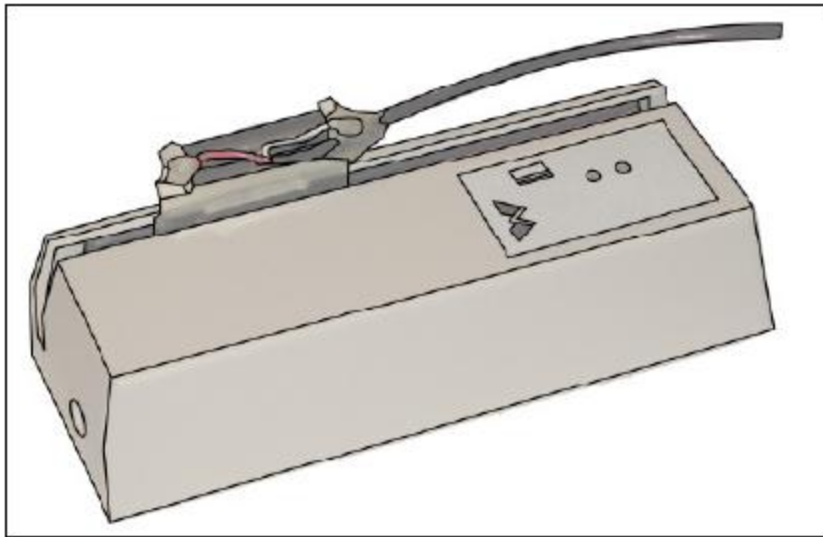
| | | | | | | | | | | | |
|---|-----------|---|---------------|---|-------------|---|-----------------|---|----------|---|-----|
| % | Site Code | ^ | Building Code | ^ | Access Code | ^ | Activation Date | ^ | End Date | ? | LRC |
|---|-----------|---|---------------|---|-------------|---|-----------------|---|----------|---|-----|

- Change data fields to common wildcard values
 - 0, 1 & 255



Attacking Access Control Systems

- Magnetic Stripe System Security
- <http://www.cs.umd.edu/~jkatz/THESES/ramsbrock.pdf>
- Thesis By: Daniel Ramsbrock, Stepan Moskovchenko & Christopher Conroy



The FRP generator's metal tab inserted in a card reader



Manual data entry and transmission



- Create custom fuzzing cards
 - Create cards with very long tracks
 - Over 80 characters on track 1
 - Over 40 characters on track 2
 - Over 107 characters on track 3
 - Mangled card formats
 - %^?LRC
 - %<=<=<=<=<=<=<=<?LRC
 - Add additional fields card



QUESTIONS?

More Information:

www.SecureState.com

www.matthewneely.com

mneely@securestate.com