Exploiting Old Mag-stripe Information with New Technology

Salvador Mendoza
Twitter: @Netxing
Blog: salmg.net
About Me

- Security Researcher
- Samsung Pay: Tokenized Numbers, Flaws and Issues
Analyzing previous talks/tools

- Major Malfunction DEFCON 14
  Magstripe Madness
- Samy Kamkar
  MagSpoof - 2015
- Weston Hecker DEFCON 24
  Hacking Hotel Keys and Point of Sale Systems
Intro to Magnetic Stripe Information

- Type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card

- TL;DR → Track1 = [UPPERCASE,numbers] Track 2/3 = Numbers

Source: samy.pl
@Netxing
Magstripe Composition

%B4929555123456789^MALFUNCTION/MAJOR^09022010100000000000000970000000?

76 Alphanumeric data characters

<table>
<thead>
<tr>
<th>SS</th>
<th>FC</th>
<th>PAN</th>
<th>FS</th>
<th>NAME</th>
<th>FS</th>
<th>ADDITIONAL DATA</th>
<th>DISCRETIONARY DATA</th>
<th>ES</th>
<th>LRC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Primary Account No. (19 digits Max.)
- Name (26 alphanumeric characters Max.)
- Expiration Date (YYMM)
- Service Code

No. of Characters: 4, 3

*PVKI
*PVV OR Offset
*CVV OR *CVC

No. of Characters: 1, 4, 3

Some or all of the above fields may be found within the Discretionary Data

Shaded area identifies control characters

- SS Start Sentinel %
- FS Field Separator ^
- FC Format Code
- LRC Longitudinal Redundancy Check Character
- ES End Sentinel ?

*(PVKI) PIN Verification Key Indicator
*(PVV) PIN Verification Value
*(CVV) Card Verification Value
*(CVC) Card Validation Code

@Netxing
Magstripe info, Parity, and Waves
Magstripe info, Parity, and Waves

<table>
<thead>
<tr>
<th>Data Bits</th>
<th>Parity</th>
<th>Character</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 0 0 1</td>
<td>0</td>
<td>0 (0H)</td>
<td>Data</td>
</tr>
<tr>
<td>1 0 0 0 0</td>
<td>1</td>
<td>1 (1H)</td>
<td>&quot;</td>
</tr>
<tr>
<td>0 1 0 0 0</td>
<td>2</td>
<td>2 (2H)</td>
<td>&quot;</td>
</tr>
<tr>
<td>1 1 0 0 0</td>
<td>3</td>
<td>3 (3H)</td>
<td>&quot;</td>
</tr>
<tr>
<td>0 0 1 0 0</td>
<td>4</td>
<td>4 (4H)</td>
<td>&quot;</td>
</tr>
<tr>
<td>1 0 1 0 0</td>
<td>5</td>
<td>5 (5H)</td>
<td>&quot;</td>
</tr>
<tr>
<td>0 1 1 0 0</td>
<td>6</td>
<td>6 (6H)</td>
<td>&quot;</td>
</tr>
<tr>
<td>1 1 1 0 0</td>
<td>7</td>
<td>7 (7H)</td>
<td>&quot;</td>
</tr>
<tr>
<td>0 0 0 1 0</td>
<td>8</td>
<td>8 (8H)</td>
<td>&quot;</td>
</tr>
<tr>
<td>1 0 0 1 1</td>
<td>9</td>
<td>9 (9H)</td>
<td>&quot;</td>
</tr>
<tr>
<td>0 1 0 1 1</td>
<td>:</td>
<td>(AH)</td>
<td>Control</td>
</tr>
<tr>
<td>1 1 0 1 0</td>
<td>;</td>
<td>(BH)</td>
<td>Start Sentinel</td>
</tr>
<tr>
<td>0 0 1 1 1</td>
<td>&lt;</td>
<td>(CH)</td>
<td>Control</td>
</tr>
<tr>
<td>1 0 1 1 0</td>
<td>=</td>
<td>(DH)</td>
<td>Field Separator</td>
</tr>
<tr>
<td>0 1 1 1 0</td>
<td>&gt;</td>
<td>(EH)</td>
<td>Control</td>
</tr>
<tr>
<td>1 1 1 1 1</td>
<td>?</td>
<td>(FH)</td>
<td>End Sentinel</td>
</tr>
</tbody>
</table>
Major Malfunction DEFCON 14

https://www.youtube.com/watch?v=ITihB1c3dHw
BlueSpoof Descendancy

MagSpoof

First Prototypes

MagSpoofPI

SamyKam

https://www.samy.pl

Designed PCB by @electronicats
Sound Amplifier
Raspberry Pi + Amplifier + Coil
Raspberry Pi - Demo
Bluetooth Technology
Bluetooth Speaker
Bluetooth Speaker
MagSpoof Cousin

BlueSpoof

MagSpoof

Electronic Cats (@electronicats) design

@Netxing
BlueSpoof
BlueSpoof tool - Characteristics

- Cheap < $20
- Easy to implement
- Escalable
- 3.7 V Battery
- Fast transmission
- Accurate
BlueSpoof - Demo

https://www.youtube.com/watch?v=elzqLhLnCek

@Netxing
Multiple Targets?

Token 1

Token 2
Controlling Multiple Speakers?

Python Sound Device Library

```
[salvador@Sal-M:/Desktop/defcon 25]$
[salvador@Sal-M:/Desktop/defcon 25]$ python -m sounddevice
> 0 Built-in Microphone, Core Audio (2 in, 0 out)
  1 Built-in Output, Core Audio (0 in, 2 out)
  2 token-, Core Audio (1 in, 0 out)
  3 token-, Core Audio (0 in, 2 out)
  4 Marsboy, Core Audio (1 in, 0 out)
< 5 Marsboy, Core Audio (0 in, 2 out)
```

https://pypi.python.org/pypi/sounddevice
Attack with Multiple Bluetooth Speakers?

https://www.youtube.com/watch?v=5hInVNLUC8s

@Netxing
Bonus Take-Away Project: iWey

@Netxing
SamyKam

https://salmg.net/2017/01/16/samykam/
Greetz, Hugs & Stuff

Samy Kamkar (@samykamkar)
Electronic Cats (@electronicats)
RMHT (raza-mexicana.org)
Los Razos!
Questions?

Salvador Mendoza
Twitter: @Netxing
Blog: salmg.net
sal@salmg.net
Thank you!

Happy Hacking Anniversary!
Resources

Samy Kamkar: samy.pl/magspoof
Electronic Cats: twitter.com/electronicats
Major Malfunction: youtube.com/watch?v=ITihB1c3dHw
Weston Hecker: youtube.com/watch?v=mV_0k9Fh590