MAGS TRIP EMAD NESS

VALID FROM 04/06
EXPIRES END 44/20
OF-3
MALFUNCTION, MAJ.

CANSECWEST 06
ISSUE DC-44-20
SORT CODE
who am i?

- security professional by day
- white hat hacker by night, weekends & when traveling..
- DEFCON goon
- DC4420 P.O.C. (London)
why mag stripe?

- old skewl
- thoroughly insecure and yet still in use
- security by obscurity (again!)
- because it's there
- i have no life
swipe cards
spot the room key...
spot the room key...
spot the ATM card...
spot the ATM card...
equipment - makstripe

- http://www.makinterface.de
- Parallel port
- Read / Write all 3 tracks
- Raw data
  - Does not care about checksums
  - Does not care about parity
- Windows support only :(（
  - not working with VMWare :(（
equipment

- http://www.sephail.net/articles/magstripe
- Audio output
  - Analyse WAV files offline
- Read all 3 tracks plus non-standard
- Raw data
  - Does not care about checksums
  - Does not care about parity
- Read only
**analysis - makstripe**

<table>
<thead>
<tr>
<th>Decode</th>
<th>Signal analysis</th>
<th>Data analysis</th>
<th>Write track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get data from</td>
<td>Total number of bits: 710</td>
<td>Examine: 6 bits per Character</td>
<td>Total parity errors: 0</td>
</tr>
<tr>
<td></td>
<td>First bit found at position: 28</td>
<td>Start with bit position: 28</td>
<td>Last valid LRC is at: 87</td>
</tr>
<tr>
<td></td>
<td>Last bit found at position: 636</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
<table>
<thead>
<tr>
<th>Char</th>
<th>Bits</th>
<th>from bit</th>
<th>to bit</th>
<th>parity</th>
<th>LRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>T2U1O0UT</td>
<td>28</td>
<td>34</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0O010110</td>
<td>35</td>
<td>41</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0061111</td>
<td>42</td>
<td>48</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1001100</td>
<td>20</td>
<td>35</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1101111</td>
<td>56</td>
<td>62</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0001001</td>
<td>69</td>
<td>69</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1001100</td>
<td>70</td>
<td>76</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1101111</td>
<td>77</td>
<td>83</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>0000001</td>
<td>84</td>
<td>90</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1000111</td>
<td>91</td>
<td>97</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>0100010</td>
<td>104</td>
<td>104</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>1010100</td>
<td>127</td>
<td>127</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>0011110</td>
<td>140</td>
<td>140</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>1111011</td>
<td>153</td>
<td>153</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>0100010</td>
<td>166</td>
<td>166</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>1010100</td>
<td>189</td>
<td>189</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>0011110</td>
<td>202</td>
<td>202</td>
<td>Ok</td>
<td></td>
</tr>
</tbody>
</table>
```

```
<table>
<thead>
<tr>
<th>Char</th>
<th>Bits</th>
<th>from bit</th>
<th>to bit</th>
<th>parity</th>
<th>LRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>00001</td>
<td>198</td>
<td>202</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>00001</td>
<td>203</td>
<td>207</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>00001</td>
<td>209</td>
<td>212</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>00001</td>
<td>213</td>
<td>217</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>00001</td>
<td>218</td>
<td>222</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>00001</td>
<td>223</td>
<td>227</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>00001</td>
<td>228</td>
<td>232</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>11111</td>
<td>233</td>
<td>237</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>01110</td>
<td>240</td>
<td>242</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>00000</td>
<td>243</td>
<td>247</td>
<td>Invalid</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>00000</td>
<td>248</td>
<td>252</td>
<td>Invalid</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>11010</td>
<td>253</td>
<td>257</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>10110</td>
<td>260</td>
<td>264</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>10000</td>
<td>263</td>
<td>267</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>00000</td>
<td>268</td>
<td>272</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>10000</td>
<td>273</td>
<td>277</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>11001</td>
<td>278</td>
<td>282</td>
<td>Ok</td>
<td></td>
</tr>
</tbody>
</table>
```
write - makstripe
standard track formats

• track 1
  - IATA – 210 BPI, 7 bit, 79 alphanumeric characters

• track 2
  - ABA – 75 BPI, 5 bit, 40 numeric characters

• track 3
  - THRIFT – 210 BPI, 5 bit, 107 numeric characters
track standards - IATA

Track 1: 210 BPI, 7 bit, 79 Alphanumeric characters
track standards - IATA

Data format
Airport
Flight No.
Day of year

Start Format From To Flight Class Day Seat Passenger End LRC
before
hotel door locks

• passive
  - all logic in the lock

• active
  - reader only
  - all logic on back-end
  - centralised alarms & reporting
passive locks

Key TYPE correct
passive locks

- Key TYPE correct
- SPECIAL key
- REJECT
- Perform SPECIAL

- Housekeeping Open
- One-Time Open
- Guest Lockout
- Crime Scene Lockout
passive locks

Key TYPE correct → SPECIAL key → Perform SPECIAL

REJECT

Correct ROOM → RESCINDED key → REJECT

NEW key → EXPIRED key
passive locks

- Key TYPE correct
- SPECIAL key
- Perform SPECIAL
- REJECT

- Correct ROOM
- RESCINDED key
- REJECT

- RESCIND previous
- NEW key
- EXPIRED key

- OPEN

Housekeeping Open
One-Time Open
Guest Lockout
Crime Scene Lockout
**keycard – multiple keys**

- ;510115352801017663012500012000000000000?8
- ;51011535280201766301250001200000000000?;

<table>
<thead>
<tr>
<th>Start</th>
<th>Property?</th>
<th>Room No.</th>
<th>Key No.</th>
<th>Magic Number?</th>
<th>Expire</th>
<th>Key Type?</th>
<th>End</th>
<th>LRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>;</td>
<td>510115</td>
<td>3528</td>
<td>01</td>
<td>01766</td>
<td>30125</td>
<td>0001200..</td>
<td>?</td>
<td>8</td>
</tr>
<tr>
<td>;</td>
<td>510115</td>
<td>3528</td>
<td>02</td>
<td>01766</td>
<td>30125</td>
<td>0001200..</td>
<td>?</td>
<td>;</td>
</tr>
</tbody>
</table>
# keycard – multiple keys

- ;51011535280101766301250001200000000000?8
- ;51011535280201766301250001200000000000?;
- ;51011535280301766301250001200000000000?:

<table>
<thead>
<tr>
<th>Start</th>
<th>Property?</th>
<th>Room No.</th>
<th>Key No.</th>
<th>Magic Number?</th>
<th>Expire</th>
<th>Key Type?</th>
<th>End</th>
<th>LRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>;</td>
<td>510115</td>
<td>3528</td>
<td>01</td>
<td>01766</td>
<td>30125</td>
<td>0001200..</td>
<td>?</td>
<td>8</td>
</tr>
<tr>
<td>;</td>
<td>510115</td>
<td>3528</td>
<td>02</td>
<td>01766</td>
<td>30125</td>
<td>0001200..</td>
<td>?</td>
<td>;</td>
</tr>
<tr>
<td>;</td>
<td>510115</td>
<td>3528</td>
<td>03</td>
<td>01766</td>
<td>30125</td>
<td>0001200..</td>
<td>?</td>
<td>;</td>
</tr>
</tbody>
</table>
### keycard – rescinding

- ;$5101150b110107004311250001200000000000\?6$
- ;$5101150b110107032311250001200000000000\?3$

<table>
<thead>
<tr>
<th>Start</th>
<th>Property?</th>
<th>Room No.</th>
<th>Key No.</th>
<th>Magic Number?</th>
<th>Expire</th>
<th>Key Type?</th>
<th>End</th>
<th>LRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>;</td>
<td>510115</td>
<td>0611</td>
<td>01</td>
<td>07004</td>
<td>31125</td>
<td>0001200..</td>
<td>?</td>
<td>6</td>
</tr>
<tr>
<td>;</td>
<td>510115</td>
<td>0611</td>
<td>01</td>
<td>07032</td>
<td>31125</td>
<td>0001200..</td>
<td>?</td>
<td>3</td>
</tr>
</tbody>
</table>
RESCINDING keys

New magic number

Lock stores last 100 keys

12345 ➔ 85123

56787

23677

...
active locks

- all locks connected to central computer
  - one wire
- checking done against live database
- key swipe as messaging system
  - room clean, out of service etc.
- security
  - access attempts
    - raise alarm!
  - audit trail
- much more expensive
  - harder to retrofit
non-standard keys
non-standard equipment
magnasee

- magnetic field visualisation
- head alignment
  - audio
  - 1/2" Tape
  - lead-in
- Carbon Tetrachloride!
  - (carbon chloride, methane tetrachloride, perchloromethane, tetrachloroethane, or benziform)
  - iron filings
  - banned as a carcinogen!! =:O
Travel on Train Companies' trains is subject to the National Rail Conditions of the conditions of carriage of other operators on whose services this ticket is not transferable. Unless otherwise stated, it may be used on any Train Company Permitted Route, and if marked “+”, on London Underground trains between stations via any recognised route appropriate to the through journey being made available for joining or alighting at an intermediate LRT Underground station.

Names of the Train Companies, copies of the National Rail Conditions of Carriage of Permitted Routes are available at Ticket Offices.

RSP No. 4599/NRES
magnasee
magnasee
size matters!

Chip and PIN is coming. Do you know your pin number?
size matters!

British Rail track is 2.5 times the width of ISO standard
size matters!

But BPI is the same...
data matters!
data analysis

• dmsb
  - decode standard track formats & character sets
  - Joseph Battaglia
    • http://www.sephail.net/articles/magstripe/

• binchop
  - aid to look for patterns and parity
  - Major Malfunction
    • http://www.alcrypto.co.uk
demonstration
making sense of the data

- character sets
attack combining

mmirda + magstripe = drinks are on me!
evolution

Key cards for mechanical, optical, magnetic stripe and smart card operated locks.

1. **Mechanical cards**: For all VingCard mechanical locking systems: 1040, 1050 and 1060 – VingCard Original.

2. **Optical cards**: For all VingCard optical electronic locking systems: 1070, 1080, 1090 and 1090e.

3. **Magnetic stripe cards**: For all VingCard magnetic stripe locking systems: 3000 and 2100 – Vision, 2100 Plus and DAVINCI.

4. **Smart cards and combination smart/magnetic stripe cards**: For all VingCard smart card locking systems – DAVINCI
next generation

- RFID
- biometric
RFID I/O tools: RFIDIOT

- [http://rfidiot.org](http://rfidiot.org) – python library
  - ISO 14443A/B
  - MIFARE Standard, MIFARE 4k, MIFARE Pro, MIFARE Ultralight, MIFARE DESFIRE, MIFARE SmartMX, SLE 55Rxx, SLE bbCL1bOS, SLE bbCLX320P, SR17b, SR1X4K, ISO14443A Tags, ISO14443B Tags, Jewel Tag (IRT0302B11 KSW DIY Eng. Sample), Sharp B, ASK GTML2ISO, TOSMART P064
  - support for ACG Dual ISO reader
    - [http://www.acg.de](http://www.acg.de)
    - no drivers required – serial device
MIFARE tags

- Block layout
- Access controls
- Demonstration

PHILIPS
mifare MF1 IC S50
Resonance Frequency: 13.56MHz
Memory: 8K Bit EEPROM memory

Please Pay For £8.00
Pre Pay
**MIFARE 1K – block layout**

<table>
<thead>
<tr>
<th>Sector 0</th>
<th>Block 0</th>
<th>Block 1</th>
<th>Block 2</th>
<th>Block 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Manufacturer block</td>
<td></td>
<td></td>
<td>Sector trailer</td>
</tr>
<tr>
<td>Sector 2</td>
<td>Block 4</td>
<td>Block 5</td>
<td>Block 6</td>
<td>Block 7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sector trailer</td>
</tr>
<tr>
<td>Sector 3</td>
<td>Block 8</td>
<td>Block 9</td>
<td>Block 10</td>
<td>Block 11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sector trailer</td>
</tr>
<tr>
<td>Sector ...</td>
<td>Block ...</td>
<td>Block ...</td>
<td>Block ...</td>
<td>Block ...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sector trailer</td>
</tr>
<tr>
<td>Sector 15</td>
<td>Block 60</td>
<td>Block 61</td>
<td>Block 62</td>
<td>Block 63</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sector trailer</td>
</tr>
</tbody>
</table>

- **Access control Block**

16 sectors, 4 blocks per sector, 16 bytes per block = 1024 bytes
manufacturer block layout

Whole block is read only

Byte: 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

Serial Number: C

Manufacturer data

Check byte

Whole block is read only
**access control block layout**

- **KeyA can never be read**
- **KeyB may be read and/or written**
  - Depending on ACB
- **ACB for various combinations**
  - Who may read/write keys
  - Who may increment/decrement/restore value blocks
data block

<table>
<thead>
<tr>
<th>Byte</th>
<th>00</th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>05</th>
<th>06</th>
<th>07</th>
<th>08</th>
<th>09</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>15</td>
<td>14</td>
<td>13</td>
<td>12</td>
<td>11</td>
<td>10</td>
<td>09</td>
<td>08</td>
<td>07</td>
<td>06</td>
<td>05</td>
<td>04</td>
<td>03</td>
<td>02</td>
<td>01</td>
<td>00</td>
</tr>
</tbody>
</table>

- 16 bytes free storage
Value block

- **Value stored 3 times**
  - Twice non-inverted, once inverted
- **Address byte stored 4 times**
  - Twice non-inverted, twice inverted
  - Audit trails
  - Backup
  - Read only (by value commands)
tag operations

Card Select → Sector Login → Read/Write etc.
demonstration
oh dear...

majormal@pirate-radio.org
http://www.alcrypto.co.uk