Sławomir Jasek
slawomir.jasek@securing.pl
@slawekja

A 2018 practical guide to hacking NFC/RFID

Confidence, Kraków, 4.06.2018
Sławomir Jasek

Enjoy appsec (dev, break, build...) since 2003.

Pentesting, consultancy, training - web, mobile, embedded...

„Smart lockpicking” trainings – HITB, HiP, Deepsec, ... www.smartlockpicking.com

Significant part of time for research.
Today

Hacking RFID is not as hard as you may think. Most common systems, practical knowledge. UID-based access control.
Cracking Mifare Classic.
Decoding the data, creating hotel „master” card.
Mobile NFC access control.
Disclaimer

These materials are for educational and research purposes only.

Do not attempt to break the law!

https://giphy.com/gifs/ZikyVyLF7aEaQ
RFID/NFC usage

Access control, hotels, car keys, attendance monitoring, race timing.
Bus, train, ski pass, football, museum tickets.
E-wallets, loyalty cards, libraries, laundries.
Contactless payments, passports, ...

Scientists develop tiny tooth-mounted sensors that can track what you eat
Wireless real-time monitoring could add precision to the linkage between diet and health

Card types, frequencies, ...

125 kHz („low frequency”) RFID
- EM4XX (Unique), HID Prox, Indala, Honeywell, AWID, ...

13.56MHz („high frequency”) NFC
- Mifare/DESFire, iCLASS, Legic, Calypso, contactless payments, ...

868MHz (UHF), other
- Vehicle id, asset tracking...
How to recognize card type? No, by the form not...
RFID implants

- Made by Dangerous Things.
- Biologically safe 2x12mm cylindrical bioglass tube
- Pre-tested and pre-loaded in sterile injection assembly
- No "anti-migration" coating means easy removal/replacement

Hack Your Body, One Implant At A Time
- Patrick Paumen

Patrick Paumen @vicarious1984, Hardwear.io 2017

https://www.youtube.com/watch?v=o5FHAm1pgWw
'Biohacker' implants travel card in hand, court says 'nice try'
An Australian man fined for not having a train ticket argued the ticket was implanted in his hand. Also, his name is Meow-Ludo Disco Gamma Meow-Meow.

by Daniel Van Boom
Updated: March 15, 2018 10:19 PM PDT
Leer en español

Your mobile phone can recognize most HF cards

125 kHz („low frequency”) RFID
- EM4XX (Unique), HID Prox, Indala, Honeywell, AWID, ...

13.56MHz („high frequency”) NFC
- Mifare/DESFire, iCLASS, Legic, Calypso, contactless payments, ...

868MHz (UHF), other
- Vehicle id, asset tracking...
ACCESS CONTROL: CARD UID
What is stored on card?

125 kHz („low frequency”) RFID
- EM41XX („Unique”)
- HID Prox II, Indala...

13.56MHz („high frequency”) NFC
- Mifare
What’s stored on the card?

The simplest cards store just individual ID

• 3-10 bytes (most often 4).
• Read-only
• Freely accessible to read
• Reader checks for registered ID.
The UID

Security: UID is set in factory and cannot be altered. Only vendor knows how to make a tag.

Guess what happened next?
Special tags – allow to change UID (starting at $0.30)

125 kHz („low frequency“) RFID
- EM41XX („Unique“)
- HID Prox II, Indala...

13.56MHz („high frequency“) NFC
- Mifare
- „MAGIC UID"

ANY UID
RFID card cloner

Low Frequency

Low + High Frequency

4 Colors Available

OBO HANDS Handheld 125KHz RFID Duplicator key copier

US $8.98 - 12.99 / piece
Free Shipping

MochuaRFID Handheld 125Khz-13.56MHZ Copier Duplicator

US $17.55 / piece
Free Shipping
RFID Cloner in action

https://www.youtube.com/watch?v=M0Z-kYL5CEU
PN532 + libnfc

NXP PN531/532/533 – one of most common HF NFC chips built in various readers, e.g. ACR122u USB (~50 EUR).

Libnfc: open source library exploiting "hidden" raw mode of NXP PN532 - useful for emulation, relay, cloning, cracking, ...

http://nfc-tools.org/index.php/Main_Page
PN532 bare modules

The cheapest ones may have antenna issues

PN532 NFC RFID module V3, NFC with Android phone extension of RFID provide Schematic and library

US $4.18 / Set

13.56mHz PN532 compatible raspberry pie / NFC card-reader

US $7.55 / piece
Our „NFC research toolkit”

PN532 board + UART USB

Magic card + tags to crack

Several NFC challenges

smartlockpicking.com/nfc-tookit
Place original card on the reader

```
root@kali:~# nfc-list
nfc-list uses libnfc 1.7.1
NFC device: pn532_uart:/dev/ttyUSB0 opened
1 ISO14443A passive target(s) found:
ISO/IEC 14443A (106 kbps) target:
    ATQA (SENS_RES): 00  04
    UID (NFCID1): 3c  3d  f1  0d
    SAK (SEL_RES): 08
```
Place „Magic” card on the reader, set new UID

```
root@kali:~# nfc-mfsetuid 3c3df10d
NFC reader: pn532_uart:/dev/ttyUSB0 opened
Sent bits:     26 (7 bits)
Received bits: 04  00
Sent bits:     93  20
Received bits: 0c  5c  ee  0d  b3
Sent bits:     93  70  0c  5c  ee  0d  b3  5c  c2
(...)
```
Banks, offices, apartments, ...

This will work in more buildings than you think...
Detecting magic cards?

Magic cards rely on special, non-standard command to unlock this feature.

- Sent bits: 50 00 57 cd
- Sent bits: 40 (7 bits)
- Received bits: a (4 bits)

(...)
Chinese answer to this problem?

Cards with direct write to manufacturer block (no special commands needed). Can also be detected.

Magic cards with one-time write!

7-byte UID? 7-byte magic card!
EMULATE CARD?
High Frequency: Chameleon Mini

Can emulate multiple HF tags

Battery-powered

99.96 EUR

http://kasper-oswald.de/gb/chameleonmini/
Chameleon: Chinese options

Starting at 45$ on Aliexpress

Multiple LEDs

Chinese manufacturer added interesting new features + GUI, recently open-sourced

https://github.com/iceman1001/ChameleonMini-rebooted/
https://github.com/iceman1001/ChameleonMini-rebootedGUI
Low Frequency: EM41XX

EM4095, starting at $2
Proxmark

Open-source FPGA hardware + software

200-300$ (depending on vendor)

proxmark.org
Proxmark „easy” – cheaper but less stable

Developed by Elechouse for Chinese market.

Fixed antennas, less memory, no external battery connector. Generally works, but sometimes problems with antennas.

Elechouse does not make it any more. Currently available on Aliexpress starting from 75$ - by other vendors, impersonating Elechouse
A new, promising player, about $100

https://www.kickstarter.com/projects/1408815241/proxmark3-rdv-40
Brute UID? In some cases it makes sense

125 kHz ("low frequency")
RFID
- Mostly random
- EM41XX ("Unique")
- HID Prox II, Indala...

13.56MHz ("high frequency")
NFC
- Mostly random
- Mifare

- Mostly sequential, may be bruted
USING SMARTPHONE?
HF (e.g. Mifare): read UID using mobile phone

Android applications:

NFC Tools:  

Mifare Classic Tool:  
HF (e.g. Mifare): read UID using mobile phone
How about emulating UID?

Not that easy...

Your phone may emulate cards (e.g. mobile payments), but by design the UID is random.

We can manipulate *NFC Controller Interface*, but it requires root.
Android: NXP NFC chip (e.g. Nexus 5X)

Modify `/etc/libnfc-nxp.conf` (requires root)

```
# Core configuration settings
NXP_CORE_CONF=( 20, 02, 2B, 0D, 
  28, 01, 00, 
  21, 01, 00, 
  30, 01, 08, 
  31, 01, 03, 
  33, 04, 01, 02, 03, 04, 
  54, 01, 06, 
  50, 01, 00, 
  5B, 01, 00, 
)
```

Note: it may depend on NFC chip firmware version.
Android Broadcom NFC chip (e.g. Nexus 5)

In /etc/libnfc-brcm-20791b05.conf, add to NFA_DM_START_UP_CFG

Length of UID (e.g. 04, 07...)

33 04 XX XX XX XX

NFA_DM_START_UP_CFG={45:CB:01:01:A5:01:01:CA:17:00:00:00:06:00:00:00:00:00:OF:00:00:00:00:
E0:67:35:00:14:01:00:00:10:B5:03:01:02:FF:80:01:01:C9:03:03:0F:AB:5B:01:00:B2:04:E8:03:00:
00:CF:02:02:08:B1:06:00:20:00:00:00:12:C2:02:00:C8:32:01:40:33:04:2C:58:E1:0D}
DEMO

https://youtu.be/94u9YSJQpFA
The same with GUI: NFC card emulator


Requires root (modifies /etc/libnfc-... files).
NFC card emulator

Put the card on the back of the phone (NFC chip location)
iPhone (jailbreak required)

Custom app, download from Cydia (3.99$):

http://limneos.net/nfcwriter
DEMO

https://youtu.be/f3LmvhHwFNc
CLONE FROM A PICTURE?
Anyone has such numbers on a tag?
EM tags with printed numbers
Decoding numbers

Example numbers on Mifare card:

0281219940 \text{ dec } = 10 \text{ C3 13 64 hex}

12784484 \text{ dec } = \text{ C3 13 64 hex}

4 bytes of UID

3 bytes of UID

sometimes inversed
**EM41XX example tag ID:** 3C009141F5

<table>
<thead>
<tr>
<th>Example number</th>
<th>Format</th>
<th>Conversion</th>
</tr>
</thead>
<tbody>
<tr>
<td>09519605</td>
<td>DEZ8</td>
<td>Last 6 hex converted to dec (9141F5 hex = 09519605 dec)</td>
</tr>
<tr>
<td>0009519605</td>
<td>DEZ10</td>
<td>Last 8 hex converted to dec</td>
</tr>
<tr>
<td>00145.16885</td>
<td>DEZ5.5</td>
<td>Digits 4-7 hex converted to dec &quot;.&quot; last 4 hex converted to dec</td>
</tr>
<tr>
<td>060.16885</td>
<td>DEZ3.5A</td>
<td>First 2 hex digits &quot;.&quot; last 4 converted to dec</td>
</tr>
<tr>
<td>000.16885</td>
<td>DEZ3.5B</td>
<td>Digits 3,4 &quot;.&quot; last 4 converted to dec</td>
</tr>
<tr>
<td>145.16885</td>
<td>DEZ3.5C</td>
<td>Digits 5,6 hex converted to dec &quot;.&quot; last 4 hex converted to dec</td>
</tr>
<tr>
<td>00257707557365</td>
<td>IK2 DEZ14</td>
<td>entire hex converted to dec</td>
</tr>
</tbody>
</table>
Possibility to clone UID from picture?

https://twitter.com/hashtag/protectyouraccesscard
#protectyouraccesscard

Tom Van de Wiele @0xtosh · 14 Sep 2017
#protectyouraccesscard And yes, the yellow post-it has his PIN on it..

https://twitter.com/0xtosh/status/908578046583635968
BTW, humans...

A blank, invalid access card for their access control.

It doesn't let you in, but the person behind you will nearly always let you in.
ICLASS
Protected identity data stored on card

125 kHz ("low frequency") RFID
- EM41XX ("Unique")
- HID Prox II, Indala...

13.56MHz ("high frequency") NFC
- Mifare
- iClass

Insecure UID: anyone can read it
iClass security

iCLASS® was specifically designed to make access control more powerful, more versatile, and more secure. All radio frequency data transmission between the tag and reader is encrypted using a secure algorithm. By using industry standard encryption techniques, iCLASS reduces the risk of compromised data or duplicated tags. For even higher security, the tag data may also be protected with DES or triple-DES encryption.

The access key is stored in reader

Only valid reader can access the data stored on card
The same key stored in every reader

Is there any problem?

„Break a single reader once and enter anywhere”

Milosch Meriac, 2010
The hack: readout protection bypass

Milosch Meriac, Henryk Plotz 2010


https://www.youtube.com/watch?v=mZNSYw9oH4Y
The iClass leaked key

3F90EBF0910F7B6F
HID iClass Master key
Thanks @Amm0nRa <3
#kiwicon
#FuckCensorship

1:39 PM - 16 Nov 2016

https://twitter.com/infosecfriends/status/799003935876870144

Not the exact form of key needed, also just the first key (allows only to clone data) to decode cleartext data you need second key
Introducing iClass SE, Seos, mobile access
By the way...

Want to learn more about readout protection?

Come visit our booth (near chill zone), I will show you how to bypass it on STM32 (one of the most common IoT microcontrollers).

Today at 15.15, tomorrow at 12:35.
Typical architecture
3 wires – black, green, white
Transmitting 1’s and 0’s

DATA0 (GREEN)

DATA1 (WHITE)

0 V

5 V

0 V

5 V

„0“

„1“
Card data transmitted: most common 26-bit

“Standard” 26Bit Wiegand Format

Facility Code (8 Bits)          Card Number (16 Bits)

P FFFFFFFFFNNNNNNNNNNNNNNNNNNN P

Leading Parity Bit (Even)      Trailing Parity Bit (Odd)

http://www.monkeyboard.org/tutorials/82-protocol/24-wiegand-converter
Typical architecture

- Most commonly cleartext bits
- Sometimes secured, or hard to clone a card
- External wall reader, quite often easy to detach

NFC
Wiegand sniffers: BLEKey
Install covertly in the reader, control from mobile app

BLEKey

Breaking Access Control with BLEKey.

http://www.blekeyrfid.com
ESP32 - wifi

RFID-Tool, $20

www.rfid-tool.com
https://github.com/rfidtool/ESP-RFID-Tool

Very similar, ESPKey:

https://github.com/octosavvi/ESPKey
RFID TOOL

ESP-RFID-Tool v1.0.4

by Corey Harding

File System Info Calculated in Bytes
Total: 2949250 Free: 2948497 Used: 753

List Exfiltrated Data
Experimental TX Mode
Configure Settings
Format File System
Upgrade Firmware
Help

https://www.youtube.com/watch?v=0o8r_ufRrFo
Best practices?

Tamper protection in readers.

Multiple layers of security - intrusion detection, monitoring, behavioral analysis, ...

OSDP (Open Supervised Device Protocol) – AES encryption, wire monitoring.
ACCESS TO CARD DATA
What is stored on card: additional data?

- **125 kHz ("low frequency")**
  - RFID
  - EM41XX ("Unique")
  - HID Prox II, Indala...
  - Just UID, no data

- **13.56MHz ("high frequency")**
  - NFC
  - Mifare
  - Other card data
Mifare Ultralight

Very common e.g. in ticketing (especially for single ticket) and hotel systems.

First Ultralight cards: no cryptographic security, just write lock protections.
Android mobile application

Android mobile application

Choose „READ” and place the tag

Scanned content
This trick works in lots of hotels!

Special „magic” card needed to change also UID (first sectors).

Only a few cards support „direct write” – possible to use with Android.
Ultralight EV1, C

Ultralight: no security

Ultralight EV1
  – Simple password (option)
  – ECC authenticity check - possible to clone using special tags

Ultralight C: 3DES
The MIFARE Classic family is the most widely used contactless smart card ICs operating in the 13.56 MHz frequency range with read/write capability.


City cards, access control, student id, memberships, internal payment, tourist card, ski pass, hotels, ...
It’s everywhere...
Mifare classic data structure

Sector = 4 blocks of 16 bytes.

Last block of a sector:
  • 2 different keys (e.g. for separate read/write)
  • access rights for the keys
Lot’s of cards use simple keys

FFFFFFFFFFFFFFF (default key)
A0A1A2A3A4A5
D3F7D3F7D3F7
000000000000
...

Using Android mobile app?

Mifare Classic Tool – free, opensource
Note: you need NXP NFC chipset (most current phones)

https://github.com/ikarus23/MifareClassicTool

Mifare Classic cracking process

- Try default, leaked keys
- Have all keys?
- YES
- Few seconds

HOORAY!

Have all keys?

Try default, leaked keys

Few seconds
Mifare Classic cracking process

Try default, leaked keys → Have all keys?

? → NO

Few seconds

? → YES

HOORAY!
Mifare Classic cracking process

Try default, leaked keys

Have all keys?

NO

Have at least one key?

YES

nested

HOORAY!
What if we could not brute the key?

„Nested” attack - exploits weakness in RNG and auth to other sector based on previous auth.

Required at least one key to any sector.

Technical details (2008):

How to exploit it?

PN532 libnfc MFOC by Nethemba  
https://github.com/nfc-tools/mfoc

Can take several minutes. Come find out yourself – it is one of our challenges!
Using proxmark?

pm3 -- hf mf nested 1 0 B fffffffffffffff d
Testing known keys. Sector count=16
[-] Chunk: 0,8s | found 29/32 keys (21)

[+] Time to check 20 known keys: 1 seconds

enter nested attack
target block: 0 key type: A
target block: 4 key type: A -- found valid key [1ab23cd45ef6]
[-] Chunk: 0,5s | found 31/32 keys (1)

target block: 0 key type: A
target block: 0 key type: A
target block: 0 key type: A
target block: 0 key type: A -- found valid key
[-] Chunk: 0,5s | found 30/32 keys (1)

[+] time in nested: 5 seconds

5 seconds (about 2s/key)
Mifare Classic cracking process

Try default, leaked keys

Have all keys?

NO

Have at least one key?

YES

nested

few sec

few min

HOORAY!
Mifare Classic cracking process

Try default, leaked keys

Have all keys?

NO

Have at least one key?

NO

YES

nested

few sec

Few seconds

few min

HOORAY!
But what if all the keys are unknown?


Libnfc: MFCUK by Andrei Costin
https://github.com/nfc-tools/mfcuk

PN532 may take 30 minutes for one key. Having one key - proceed with „nested”.
Mifare Classic cracking process

Try default, leaked keys

Have all keys?

No

Have at least one key?

No

darkside

30 sec

30-60 min

YES

cracked 1 key

nested

few sec

few min

YES

HOORAY!
Mifare EV1 – „hardened”

The „nested” and „darkside” attacks exploit implementation flaws (PRNG, side channel, ...).

Mifare Classic EV1, Plus in Classic mode (SL1) – fixes the exploit vectors.
Hardnested libnfc


PN532 libnfc: miLazyCracker - automatically detects card type, proceeds with relevant attack scenario:
https://github.com/nfc-tools/miLazyCracker
https://www.youtube.com/watch?v=VcU3Yf5AqQI
Mifare Classic hardened (Plus SL1, EV1) cracking

Try default, leaked keys

Have all keys?

NO

Have at least one key?

YES

PN532

Several min

PN532

hardnested

HOORAY!
Mifare Classic hardened (Plus SL1, EV1) cracking

Try default, leaked keys

Have all keys?

No

Have at least one key?

No

Yes

hardnested

Several min

No

HOORAY!
EV1 with all sectors secured?

„Hardnested“ requires at least one known key. What if all the keys are unknown?

Recover the key using online attack (mfkey) – requires to emulate/sniff the card to a valid reader.

Hardware: Proxmark, Chameleon Mini RevE „Rebooted“
Chameleon Mini reader attack

1. Set MF_DETECTION
2. Place the Chameleon at reader
3. Download dump
4. „Reckon“ (mfkey) – cracks the key
Mifare Classic hardened (Plus SL1, EV1) cracking

Try default, leaked keys

Have all keys?

NO

Have at least one key?

NO

Hardnested

Several min

YES

NO

Reader attack

Trip to the reader

PN532

Few seconds

YES

HOORAY!
Final NXP recommendation to upgrade (2015.10)

NXP is recommending that existing MIFARE Classic® systems are upgraded. Furthermore, NXP does not recommend to design in MIFARE® Classic in any security relevant application.

Some workarounds (do not fix the problem)

Make the attack more difficult
- Use EV1 with all sectors secured, diversified keys per card
- One way counters, timestamps, special access rights
- Encrypt/sign/hash card content
- Online verification
- Other tricks
Migrate to more secure Mifare Plus, DESFire, ...

More powerful chip built-in: DES, AES, ...

No currently known attacks.

Configure properly!

• Preferably individual key for each user.

• There are systems that use DESFire but check only for UID ;)

https://twitter.com/FailsWork/status/984855234953564160
CARD CONTENT
Card content

Data stored on card is often encoded – e.g. scrambled using individual card UID.
Hotel: 2 cards for the same room

Card UID

Encoded access data?

Checksum?

http://blog.j-michel.org/post/77378532178/rfid-when-the-manufacturer-matters
The encoded data

<table>
<thead>
<tr>
<th>Card 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>7E  EE  5F  71 06  FC  90  F6  A9  F9  7D  7E  C6  7D  E2  60  7E</td>
</tr>
<tr>
<td>BE  81  7E  FF  7E  42  7E  7E  7E  7E  7E  7E  7E  7E  7E  7E</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Card 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>82  12  A3  8D  FA  C0  2B  8B  55  05  81  82  3A  81  1E  9C  82</td>
</tr>
<tr>
<td>42  7D  82  03  82  BE  82  82  82  82  82  82  82  82  82  82</td>
</tr>
</tbody>
</table>
## The encoded data

### Card 1

<table>
<thead>
<tr>
<th>7E</th>
<th>EE</th>
<th>5F</th>
<th>71</th>
<th>06</th>
<th>FC</th>
<th>90</th>
<th>F6</th>
<th>A9</th>
<th>F9</th>
<th>7D</th>
<th>7E</th>
<th>C6</th>
<th>7D</th>
<th>E2</th>
<th>60</th>
<th>7E</th>
</tr>
</thead>
<tbody>
<tr>
<td>BE</td>
<td>81</td>
<td>7E</td>
<td>FF</td>
<td>7E</td>
<td>42</td>
<td>7E</td>
<td>7E</td>
<td>7E</td>
<td>7E</td>
<td>7E</td>
<td>7E</td>
<td>7E</td>
<td>7E</td>
<td>7E</td>
<td>7E</td>
<td></td>
</tr>
</tbody>
</table>

### Card 2

<table>
<thead>
<tr>
<th>82</th>
<th>12</th>
<th>A3</th>
<th>8D</th>
<th>FA</th>
<th>C0</th>
<th>2B</th>
<th>8B</th>
<th>55</th>
<th>05</th>
<th>81</th>
<th>82</th>
<th>3A</th>
<th>81</th>
<th>1E</th>
<th>9C</th>
<th>82</th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>7D</td>
<td>82</td>
<td>03</td>
<td>82</td>
<td>BE</td>
<td>82</td>
<td>82</td>
<td>82</td>
<td>82</td>
<td>82</td>
<td>82</td>
<td>82</td>
<td>82</td>
<td>82</td>
<td>82</td>
<td></td>
</tr>
</tbody>
</table>

- Repeating 7E
- Repeating 82

**Maybe there were 00’s in cleartext?**
XOR

\[ \begin{array}{c}
7E & EE & 5F & 71 & 06 & FC & 90 & F6 & A9 & F9 & 7D & 7E & C6 & 7D & E2 & 60 & 7E \\
BE & 81 & 7E & FF & 7E & 42 & 7E & 7E & 7E & 7E & 7E & 7E & 7E & 7E & 7E & 7E \\
\end{array} \]

\[\begin{array}{c}
7E & 7E & 7E & 7E & 7E & 7E & 7E & 7E & 7E & 7E & (\ldots) \end{array}\]

= 

\[ \begin{array}{c}
00 & 90 & 21 & 0F & 78 & 82 & EE & 88 & D7 & 87 & 03 & 00 & B8 & 03 & 9C & 1E & 00 \\
C0 & FF & 00 & 81 & 00 & 3C & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\
\end{array} \]
Same room: card 1 XOR 7E; card 2 XOR 82

00 90 21 0F 78 82 EE 88 D7 87 03 00 B8 03 9C 1E 00 C0
FF 00 81 00 3C 00 00 00 00 00 00 00 00 00 00 00

00 90 21 0F 78 42 A9 09 D7 87 03 00 B8 03 9C 1E 00 C0
FF 00 81 00 3C 00 00 00 00 00 00 00 00 00 00 00
Same room: card 1 XOR 7E; card 2 XOR 82

Now just a few bytes differ
First public initial reverse of Vingcard

Jean-Michel Picod, 2014

http://blog.j-michel.org/post/77378532178/rfid-when-the-manufacturer-matters

http://blog.j-michel.org/post/85755629755/rfid-followup-on-vingcard
Vingcard hack – 2018.04

„Ghost in the locks” Infiltrate 2018, Tomi Tuominen and Timo Hirvonen

https://vimeo.com/267613809

Collect various hotel cards...

Mikko Hypponen @mikko · Feb 26
Found a way to visualize my flight patterns.
This is 2017.

I played a small part in the research, by collecting hotel room keycards for Tomi & Timo to hack.

https://twitter.com/mikko/status/968067739414925312

https://twitter.com/mikko/status/989154230723334151
Get the hotel software

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vision 6.3 Total CD .zip</td>
<td>27-May-2014 13:56 186M</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ghost in the locks, Tomi Tuominen, Timo Hirvonen, INfiltrate 2018, [https://vimeo.com/267613809](https://vimeo.com/267613809)
And its license...

Serial number spotted in software manual ;)

The „master” card

Create it using the software? Does not work for real hotel – individual keys.

Get real „master” card, and fuzz?

Turns out: having any guest card for a given hotel, it takes just a short brute-force to create master key.
Attack

Other hotel system: guest card data

I checked in yesterday evening.

Can you tell me the check out date and time?

How about the room number?
Hotel guest card data

Check in: 2018.06.03
20:47

Check out: 2018.06.13
15:00

Room number: 114
„Master” card?

Having just a guest card for any hotel using this system, I can create „master” card in about a minute.

I’m sorry I won’t tell you how to do it – it looks like the vendor will not patch ;)

4-star hotel – unlock all the doors like a boss!
I’m really sorry but I could not resist...

remote Jeep exploit

Vingcard master card

oh, just kidding ;}
By the way

Vendor lists several hundred hotels implementing this system on the website.

Browse by country, hotel type, name, pictures ...

No, I won’t give it to you either ;)
Crime scene card?

Special card that locks the door permanently – no one can enter, not even master/emergency card.

The police has to force the door open (break it).
Real risk?

Some hotels still use even more legacy systems.

Monitoring, guards, additional layers of security...
On the other hand...

A readout of activity that took place on the hotel room's electronic door lock indicated that an attempt was made to reprogram al-Mabhouh's electronic door lock at this time. The investigators believe that the electronic lock on al-Mabhouh's door may have been reprogrammed and that the killers gained entry to his room this way. The locks in question, VingCard Locklink brand, can be accessed and reprogrammed directly at the hotel room door.

thanks Tomi Tuominen & Timo Hirvonen for digging it

https://www.wired.com/2017/08/the-hotel-hacker/
City cards?

Metrodroid: Android app to read (NOT edit) city card data.

https://github.com/micolous/metrodroid/

Finding the balance

$ vbindiff gocard-2015xxxx_yyyy.mfc gocard-2015xxxx_yyyy.mfc

https://www.youtube.com/watch?v=qVvNdfKRw7M
City cards fraud?

Aplikacja do nielegalnego ładowania Warszawskiej Karty Miejskiej za BTC

By Dmitry Bestuzhev on October 21, 2014. 4:39 pm

Tarjeta BIP! is the electronic payment system used in Chile to pay for public transportation via NFC incorporated in the user’s smartphone. Numerous projects enabling mobile NFC ticketing for public transportation have been already executed worldwide. This is a trend. It means that criminal minds should be interested in it. Moreover, they are.

More and more people keep talking about the feature of payments via NFC. The problem in this particular case is that somebody reversed the "Tarjeta BIP!" cards and found a means to re-charge them for free. So, on Oct. 10 the very first widely-available app for Android appeared, allowing users to load these transportation cards with 10k-Chilian pesos, a sum equal to approximately $17 USD.


Nathan Jeffrey-Payne, 28, of Nutfield Gardens, Seven Kings, was part of a six-strong gang of sophisticated criminals who found a way to clone older Oyster cards and trick ticket machines into thinking there was still money on them.

These fraudulent first generation Oysters were then used at multiple ticket machines across London to obtain thousands of pounds in false refunds.
MOBILE ACCESS
Evolution goes mobile
Host Card Emulation

Software emulates contactless smart card.

Mobile OS provides interface for communication, the same technology used for contactless payments.

(See also my last year’s HCE security talk).
Apple is making a significant change to a wireless chip in the iPhone that will allow users to more securely unlock doors enabled with the same technology, a person familiar with the matter said.
How does it work? (most cases)

Mobile app

NFC

WIEGAND?
How does it work? (most cases)

Mobile app stores:
- Key to the reader (usually per-installation)
- Individual user ID
What could possibly go wrong?

Mobile malware – steals the access data.

Malicious user – tampers his own ID and gets access to restricted areas.

Administrative access – reader reconfiguration.

More info soon...
New possibility to make it right?

End-to-end encryption, individual asymmetric keys, mutual auth, ...

New backend
Not easy to get such system...

Hello Slawomir,

I will be completely honest with you. Today I stumbled upon your website, and I briefly read through some of the articles.
Time...
Risk?

- Impact
- Probability/ease of exploitation
- Conditions to exploit
- Time
Design the system properly?

Own crypto is usually a bad idea.

The design of a system should not require secrecy.

The exploit may be non-obvious, and attack conditions will change in time.
Want to try tricks yourself?

Come visit our booth to win NFC toolset, play with our installations, clone the cards and crack our NFC challenges!

smartlockpicking.com/nfc-tookit

Also several mini-shows.
Want to learn more?

Trainings
Tutorials
Events

Next up: HackInParis,
25-29.06.2018

https://www.smartlockpicking.com
Thank you! Questions?

Slawomir.Jasek@securing.pl  slawekja