securing

<15 yrs>

Slightly edited version of the slightly edited original photo :)
https://vimeo.com/267613809

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

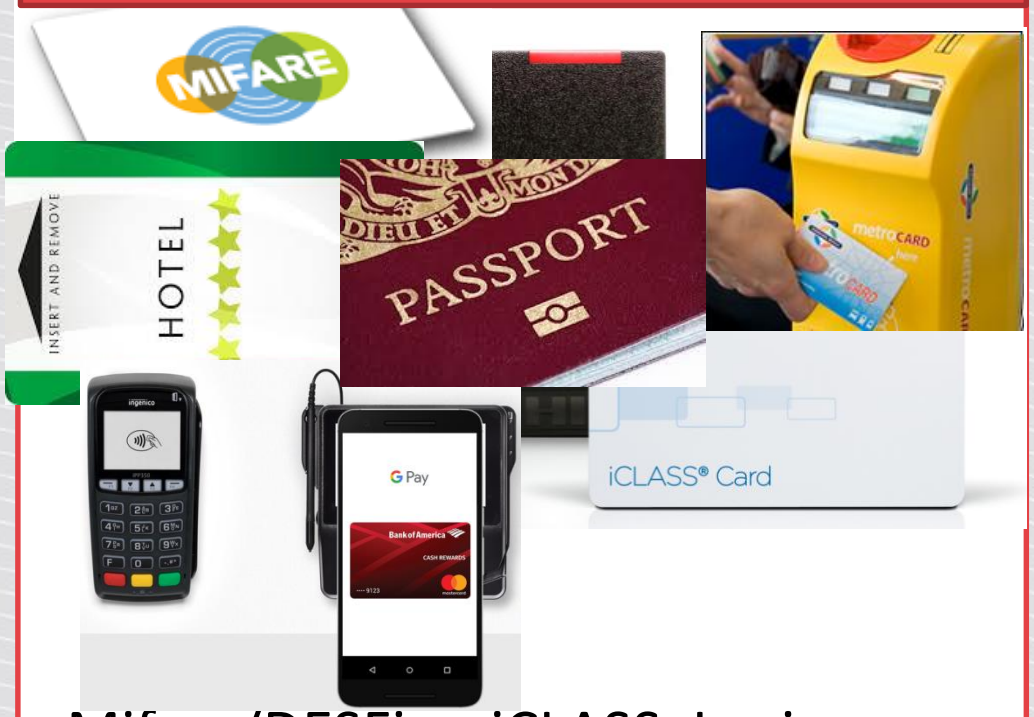
https://now.tufts.edu/news-releases/scientists-develop-tiny-tooth-mounted-sensors-can-track-what-you-eat

Card types, frequencies, ...

125 kHz („low frequency”) RFID

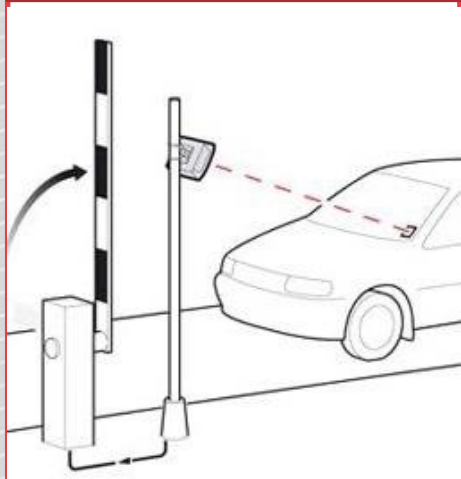
EM4XX (Unique), HID Prox, Indala, Honeywell, AWID, ...

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

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

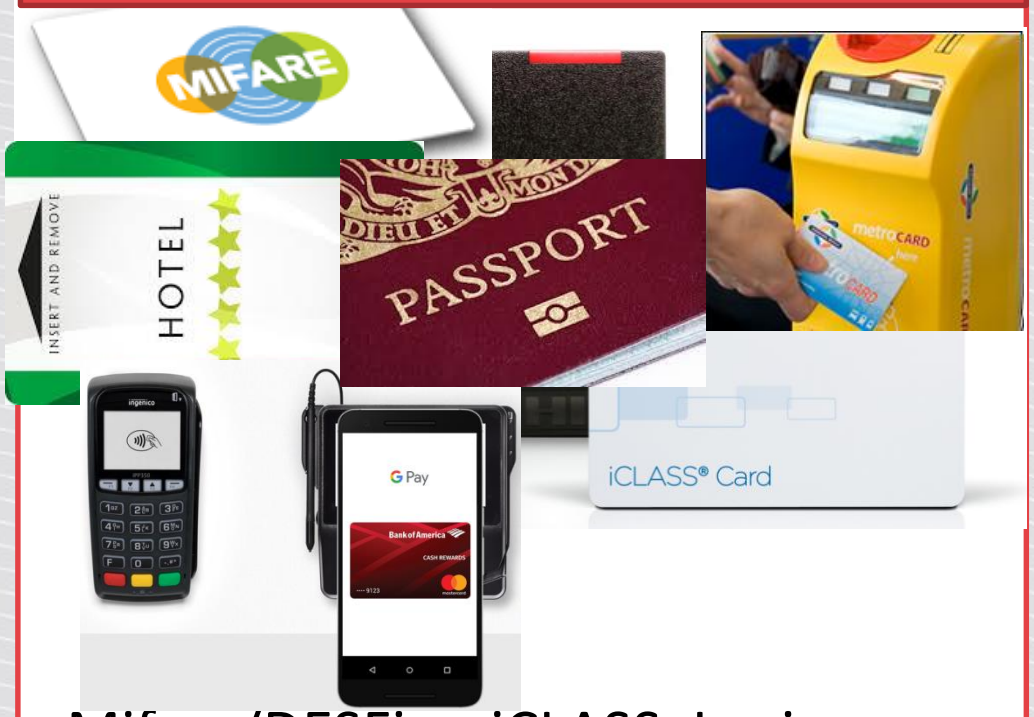
https://www.cnet.com/google-amp/news/biohacker-implants-travel-card-in-hand-court-says-nice-try/

Your mobile phone can recognize most HF cards

125 kHz („low frequency”) RFID

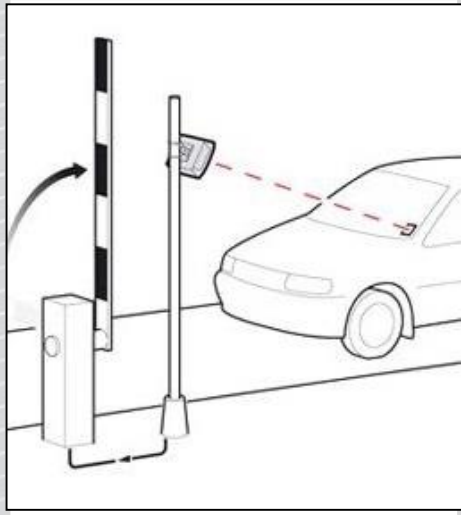
EM4XX (Unique), HID Prox, Indala, Honeywell, AWID, ...

13.56MHz („high frequency”) NFC



Mifare/DESFire, iCLASS, Legic, Calypso, contactless payments, ...

868MHz (UHF), other

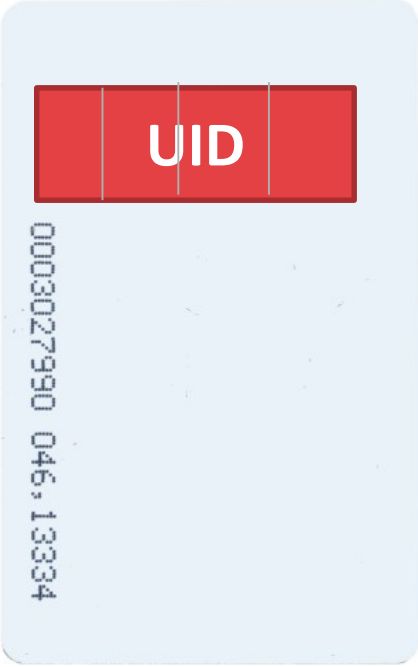


Vehicle id, asset tracking...

ACCESS CONTROL: CARD UID

What is stored on card?

125 kHz („low frequency”) RFID



EM41XX („Unique”)

HID Prox II, Indala...

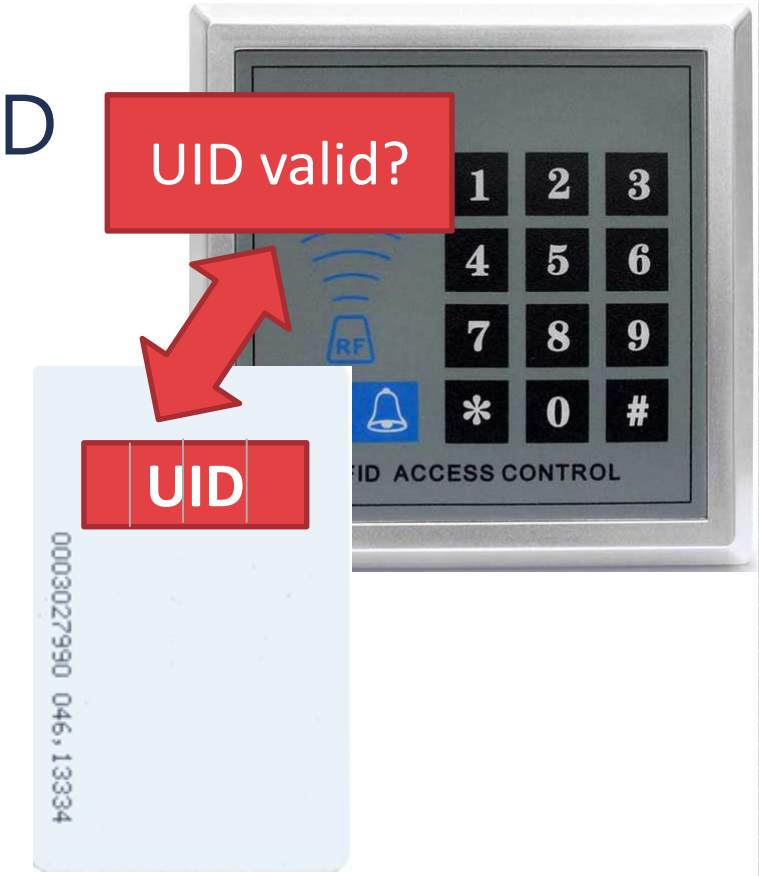
13.56MHz („high frequency”) NFC

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

RFID card cloner

Low Frequency

4 Colors Available

OBO HANDS Handheld 125KHz **RFID** Duplicator key copier

US $8.98 - 12.99 / piece
Free Shipping

Low + High Frequency

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
```

Card UID

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, …

https://giphy.com/gifs/iI6eeGjwScTCM

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)
(...)
```

It is possible to detect and discard such cards.

https://giphy.com/gifs/security-yPICcTU83NTJm

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

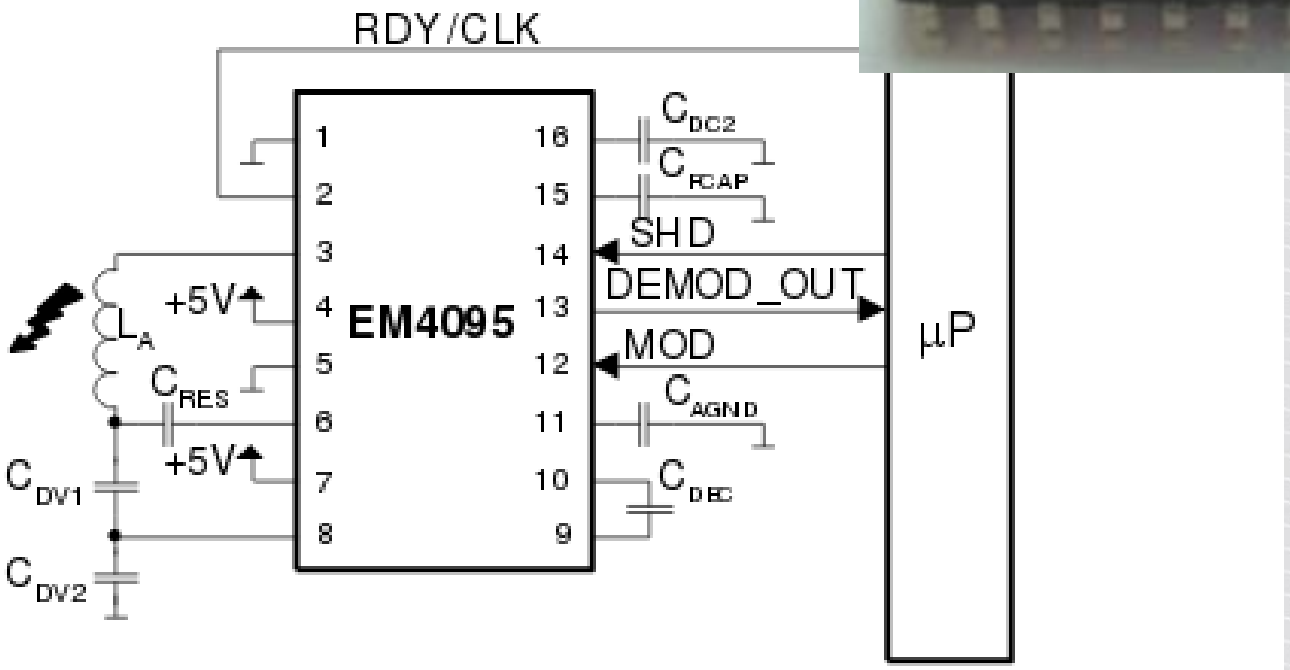
Chinese manufacturer added interesting new features + GUI, recently open-sourced

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.

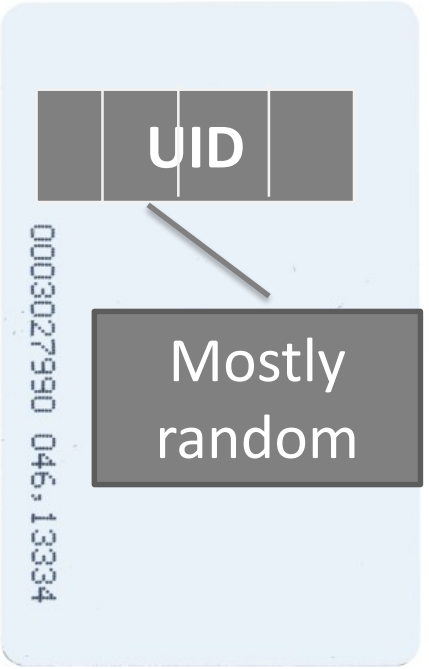
Elechouse does not make it any more. Currently available on Aliexpress starting from 75$ - by other vendors, impersonating Elechouse

A new, promising player, about $100

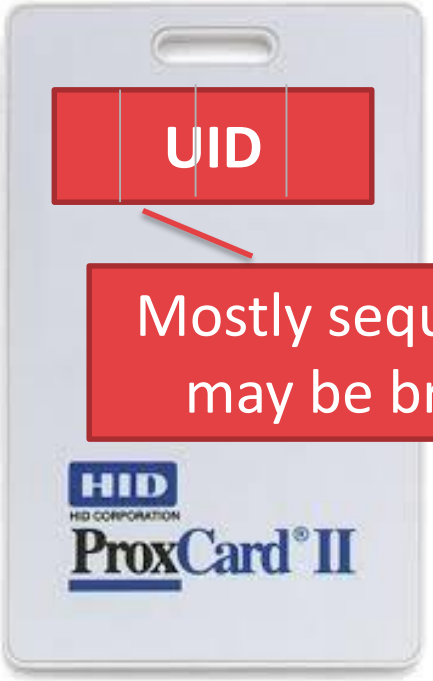
https://www.kickstarter.com/projects/1408815241/proxmark3-rdv-40

Brute UID? In some cases it makes sense

125 kHz („low frequency”) RFID



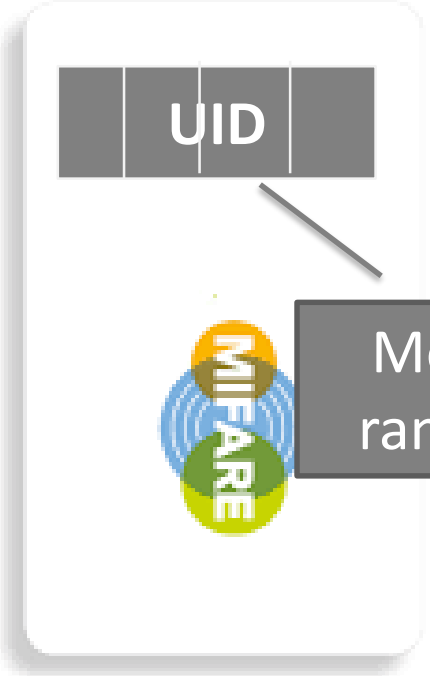
EM41XX („Unique”)



HID Prox II, Indala...

Mostly sequential, may be bruted

13.56MHz („high frequency”) NFC



Mifare

USING SMARTPHONE?

HF (e.g. Mifare): read UID using mobile phone

Android applications:

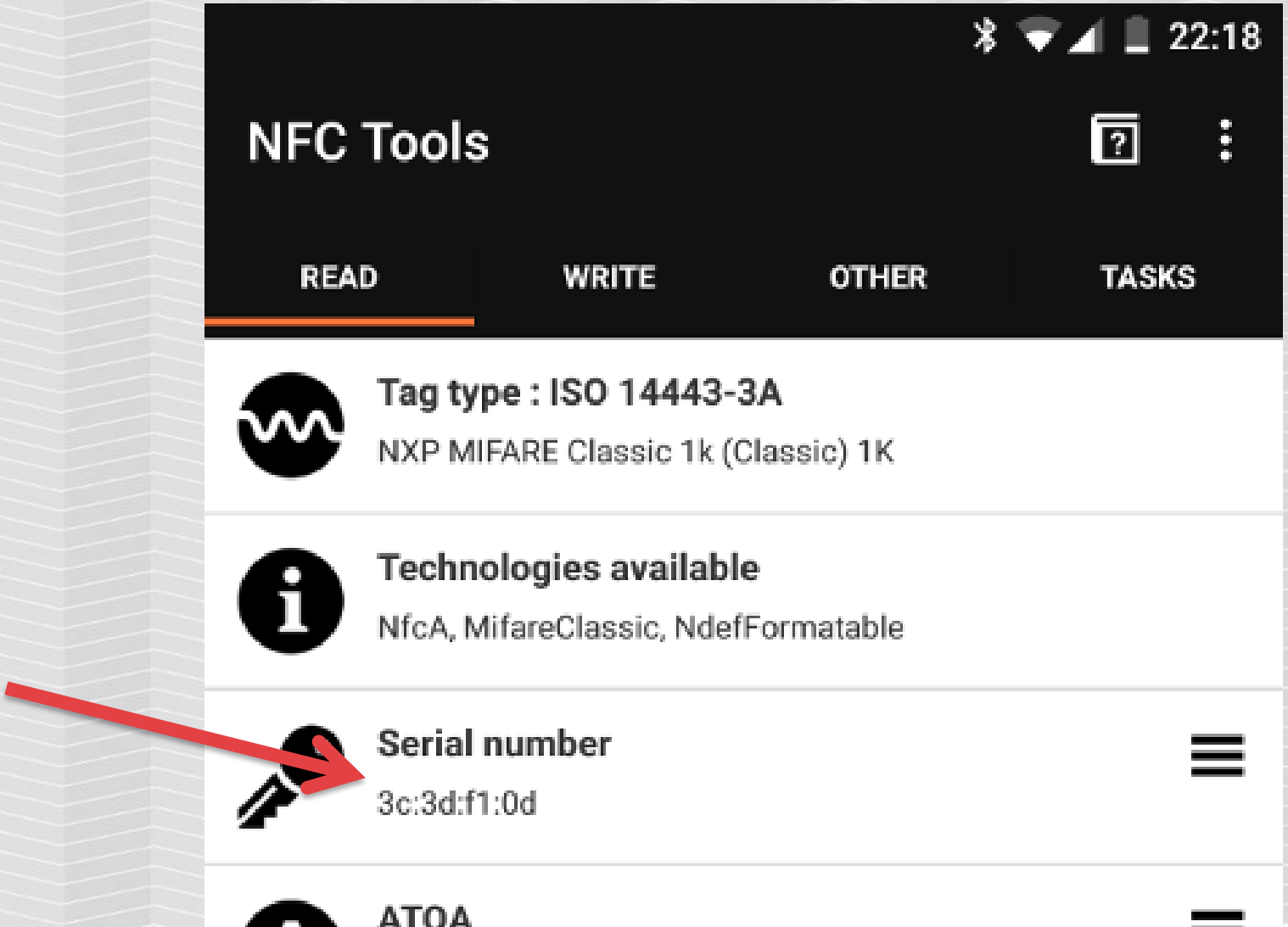
NFC Tools:

https://play.google.com/store/apps/details?id=com.wakdev.wdnfc

Mifare Classic Tool:

https://play.google.com/store/apps/details?id=de.syss.MifareClassicTool

HF (e.g Mifare): read UID using mobile phone

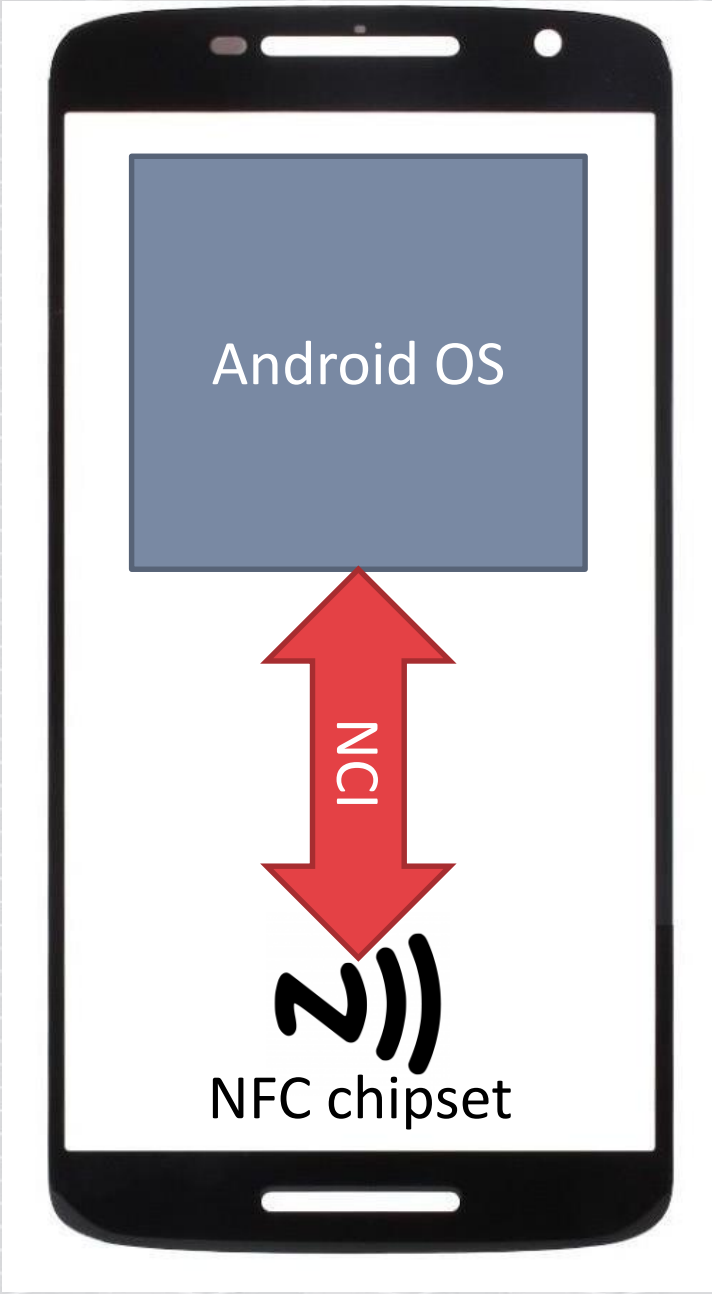


How about emulating UID?

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,
```

Put your UID here

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

NCI parameter

Your UID

```
NFA_DM_START_UP_CFG={45:CB:01:01:A5:01:01:CA:17:00:00:00:00:06:00:00:00:00:0F: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

https://play.google.com/store/apps/details?id=com.yuanwofei.cardemulator

NFC Card Emulator

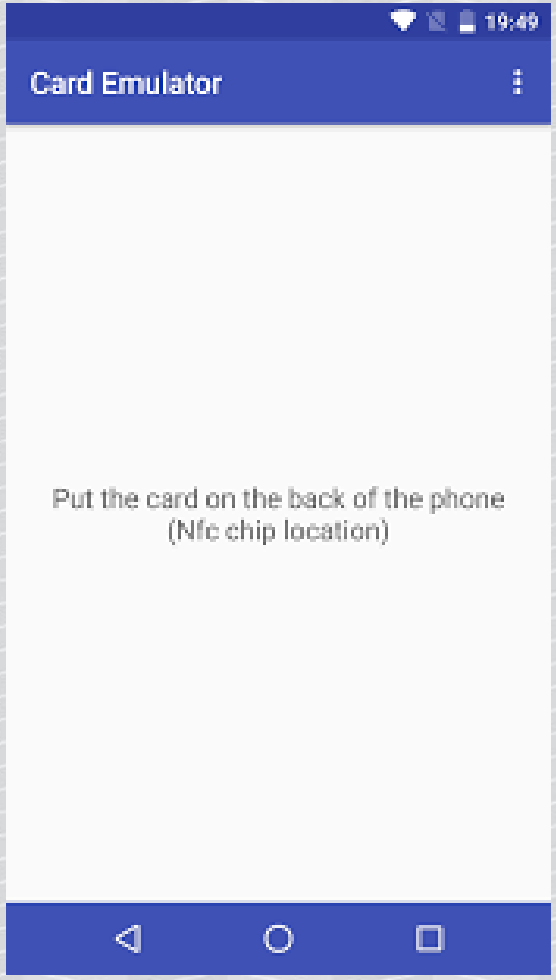
yuanwofei Tools

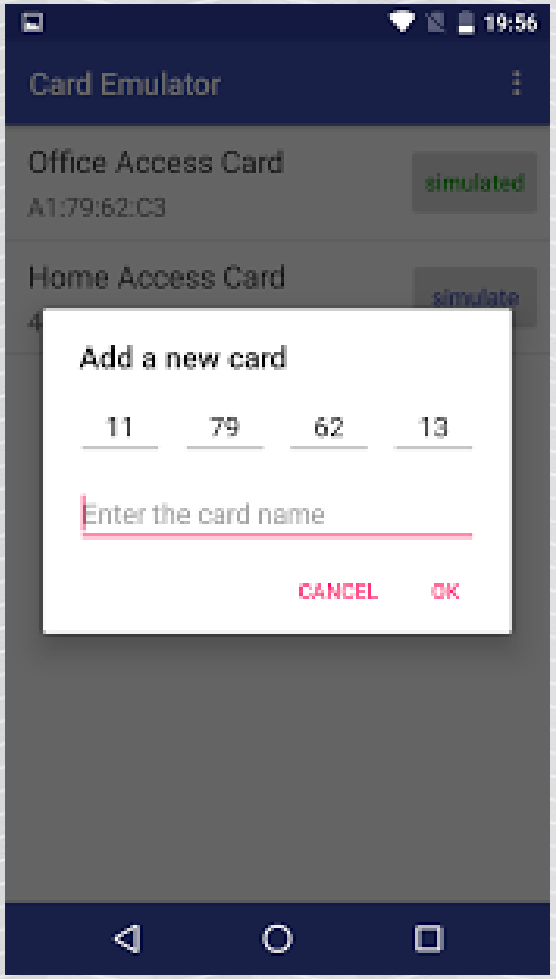
PEGI 3

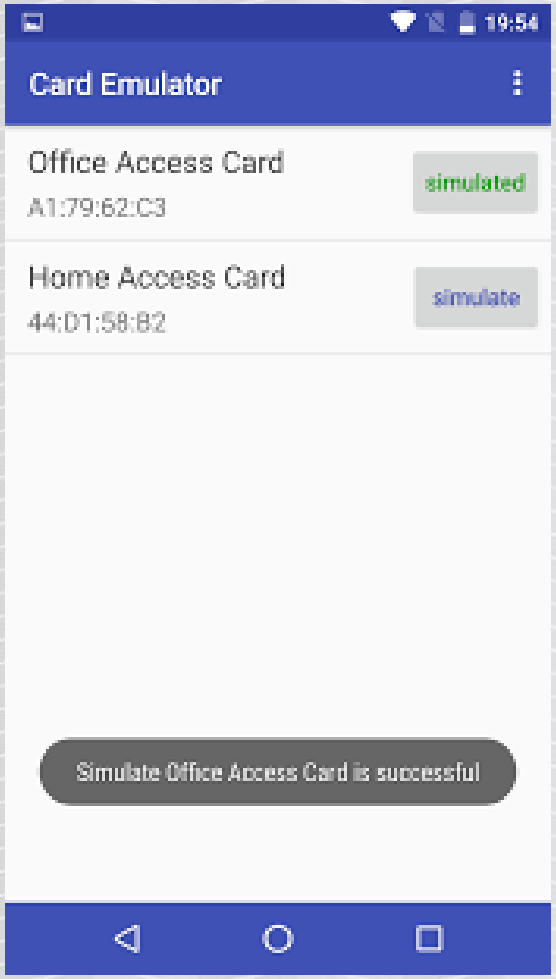
You don't have any devices

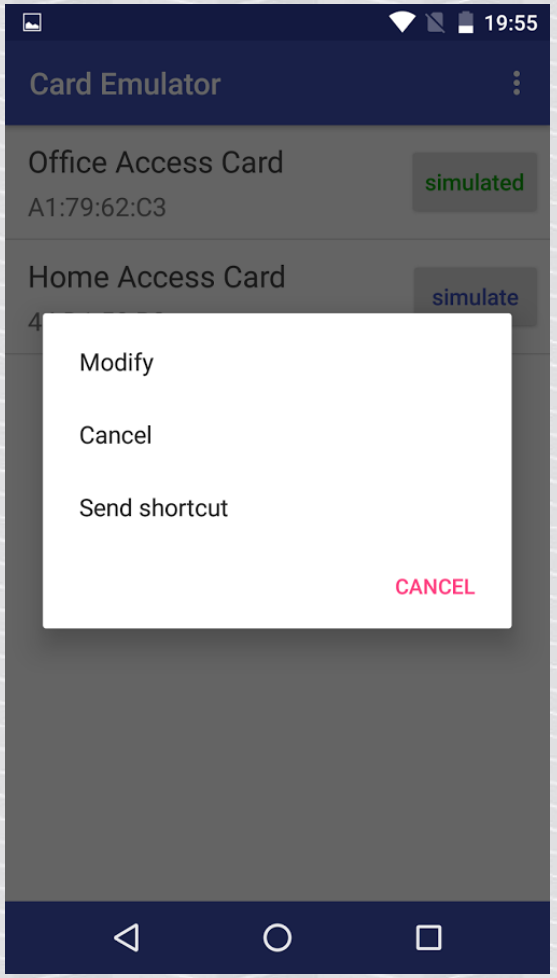
Requires root (modifies /etc/libnfc-... files).

NFC card emulator





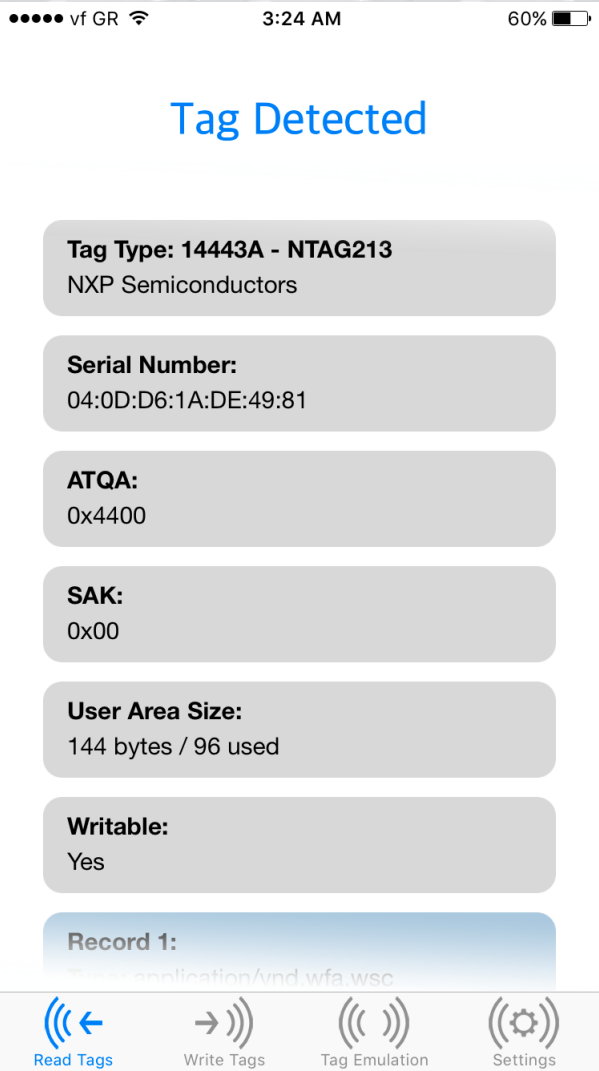


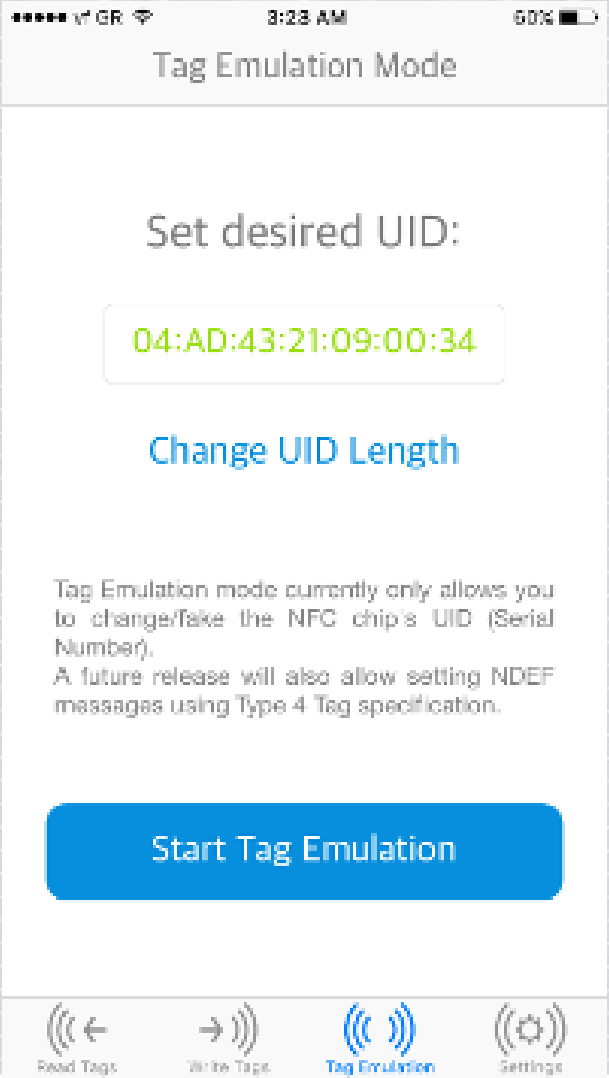


iPhone (jailbreak required)

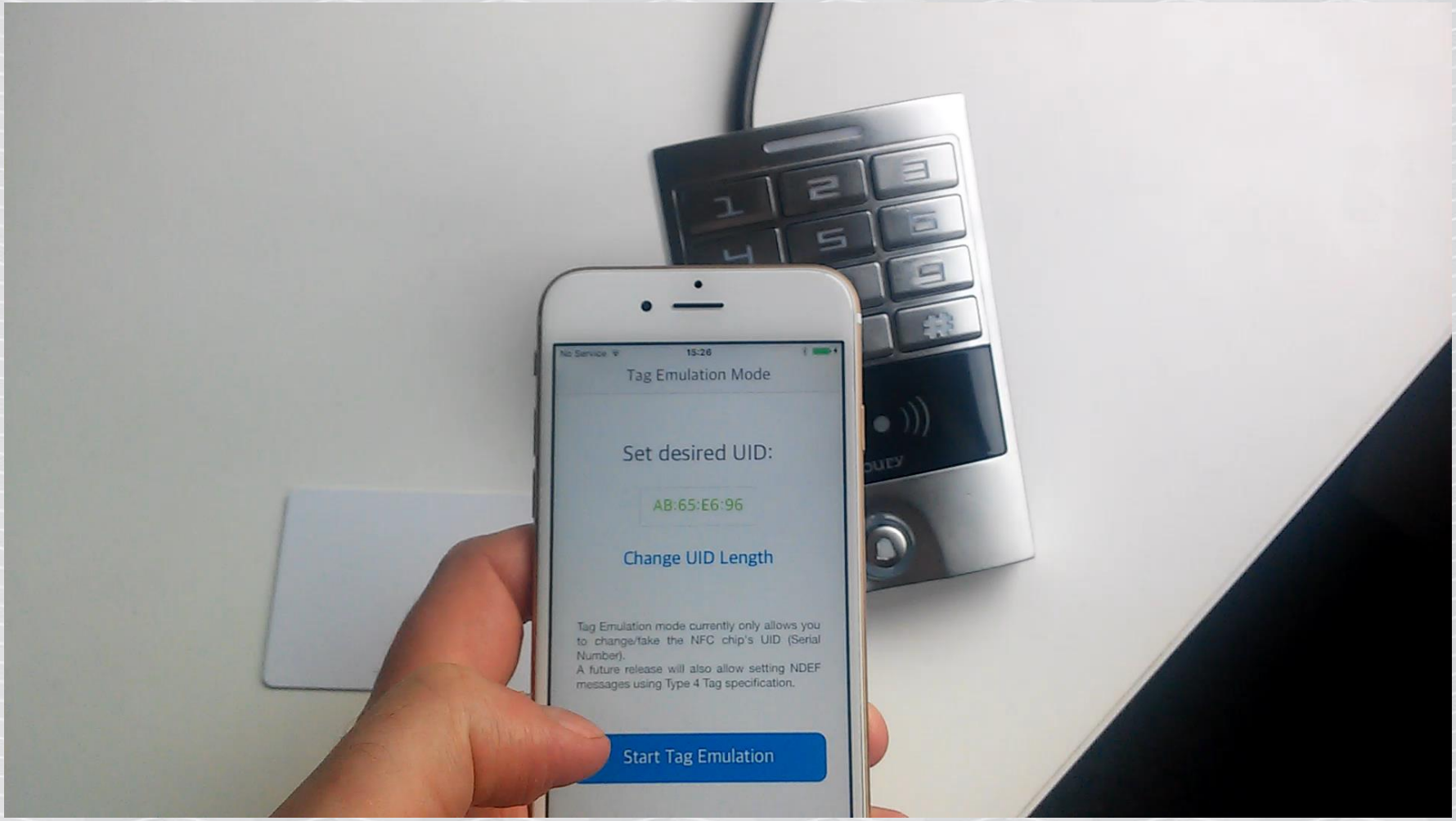
Custom app, download from Cydia (3.99$):

http://limneos.net/nfcwriter





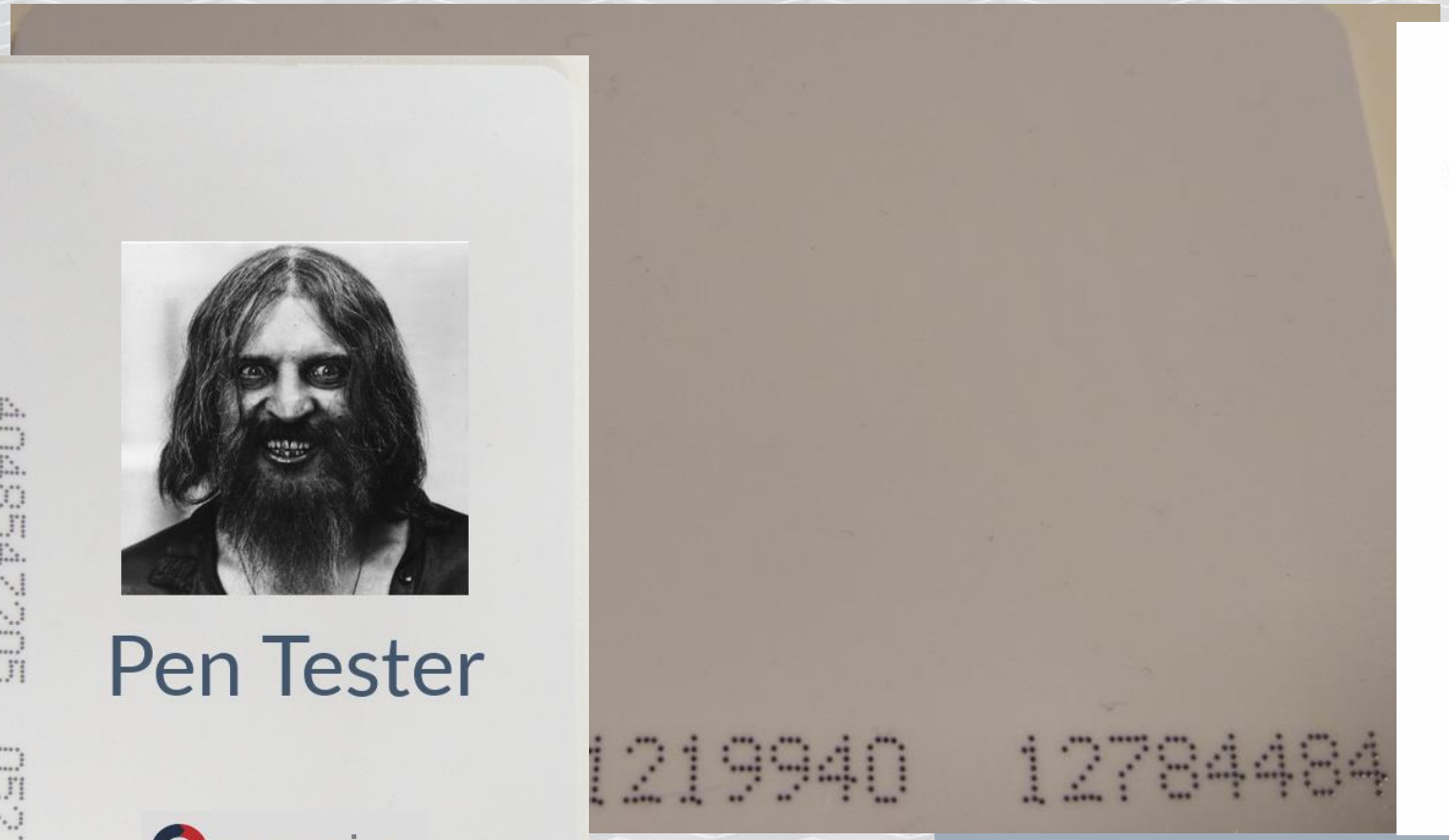
DEMO

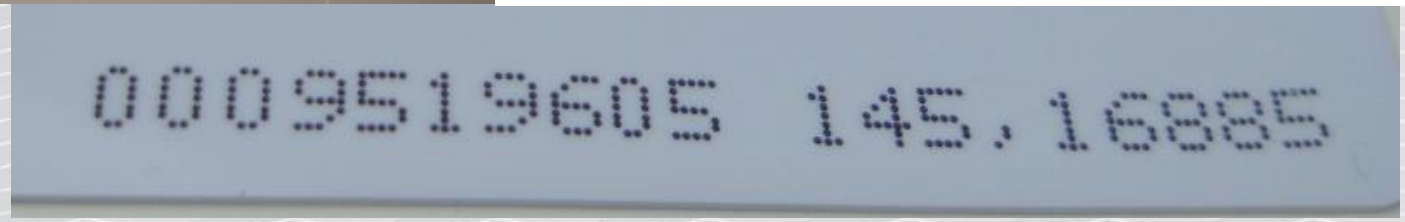


https://youtu.be/f3LmvhHwFNc

CLONE FROM A PICTURE?

Anyone has such numbers on a tag?

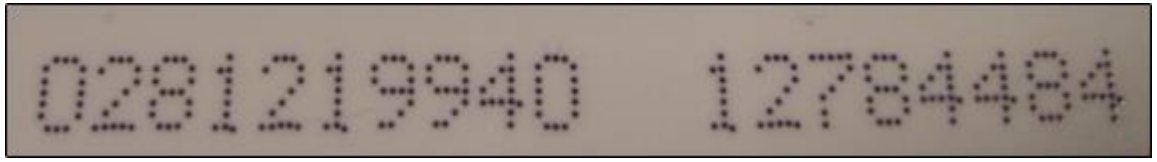




EM tags with printed numbers

Decoding numbers

Example numbers on Mifare card:

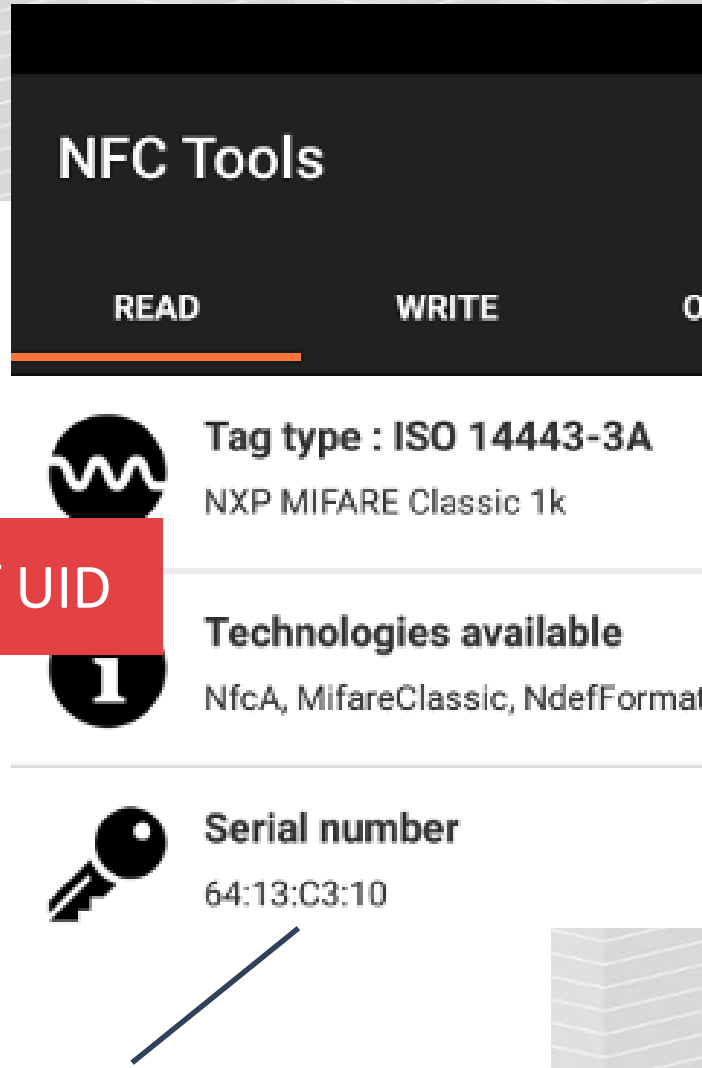


4 bytes of UID

0281219940 dec = 10 C3 13 64 hex

12784484 dec = C3 13 64 hex

3 bytes of UID



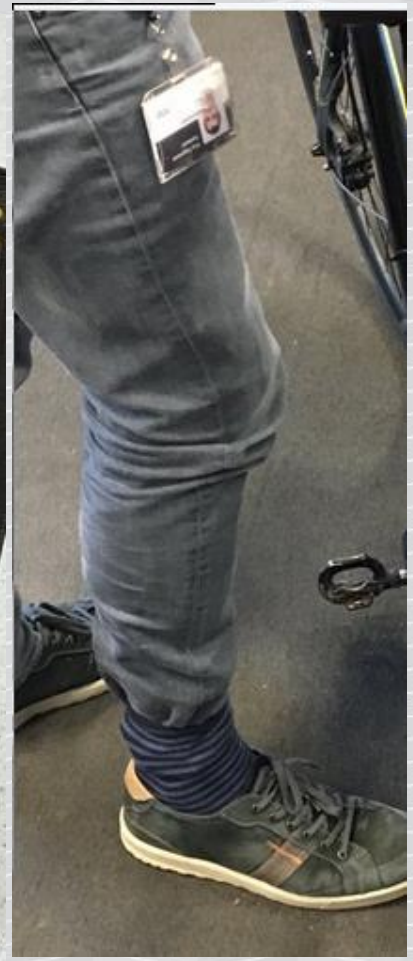
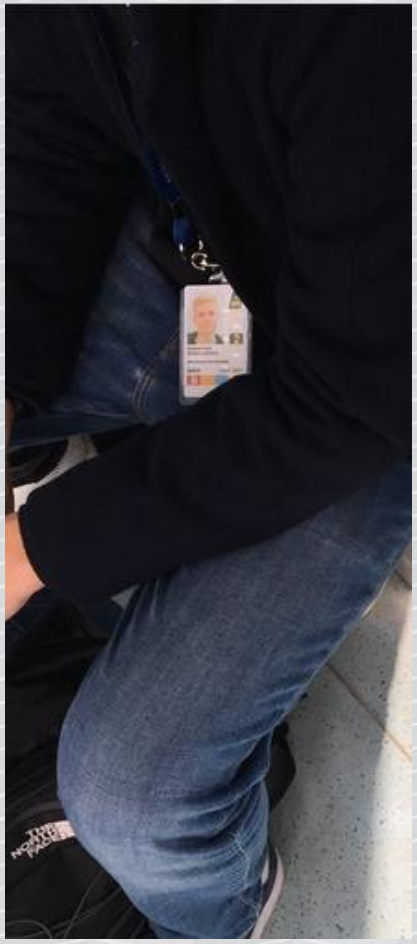
sometimes inversed

EM41XX example tag ID: **3C009141F5**

Example number	Format	Conversion
09519605	DEZ8	Last 6 hex converted to dec (9141F5 hex = 09519605 dec)
0009519605	DEZ10	Last 8 hex converted to dec
00145.16885	DEZ5.5	Digits 4-7 hex converted to dec "." last 4 hex converted to dec
060.16885	DEZ3.5A	First 2 hex digits "." last 4 converted to dec
000.16885	DEZ3.5B	Digits 3,4 "." last 4 converted to dec
145.16885	DEZ3.5C	Digits 5,6 hex converted to dec "." last 4 hex converted to dec
00257707557365	IK2 DEZ14	entire hex converted to dec

Possibility to clone UID from picture?




https://twitter.com/hashtag/protectyouraccesscard

#protectyouraccesscard

https://twitter.com/0xtosh/status/908578046583635968

BTW, humans...

the cybergibbons @cybergibbons · May 23

A blank, invalid access card for their access control.

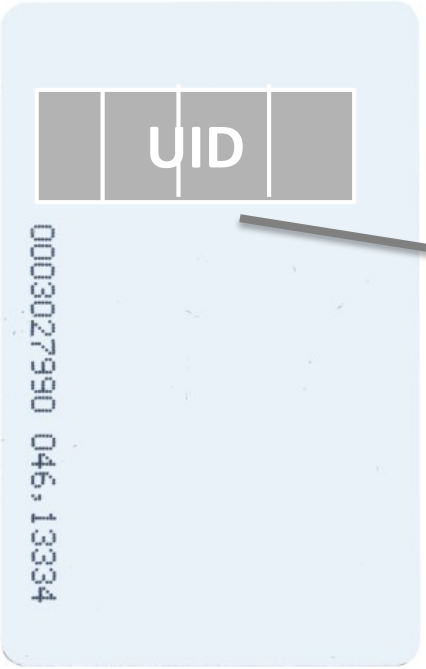
It doesn't let you in, but the person behind you will nearly always let you in.

https://twitter.com/cybergibbons/status/999283915218128896

ICLASS

Protected identity data stored on card

125 kHz („low frequency”) RFID



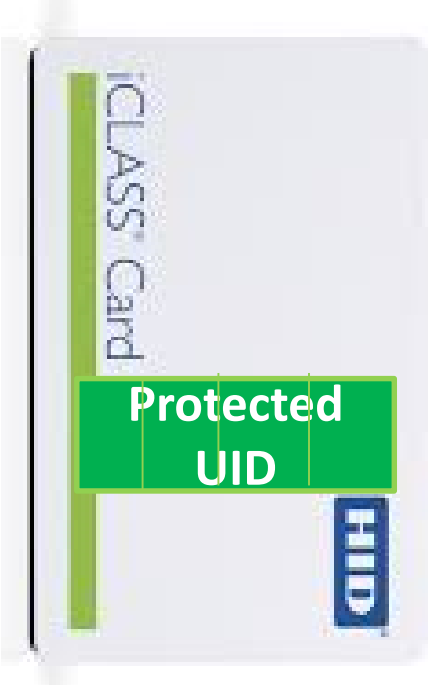
EM41XX („Unique”)

HID Prox II, Indala...

Insecure UID
anyone can read it

13.56MHz („high frequency”) NFC

Mifare



iClass

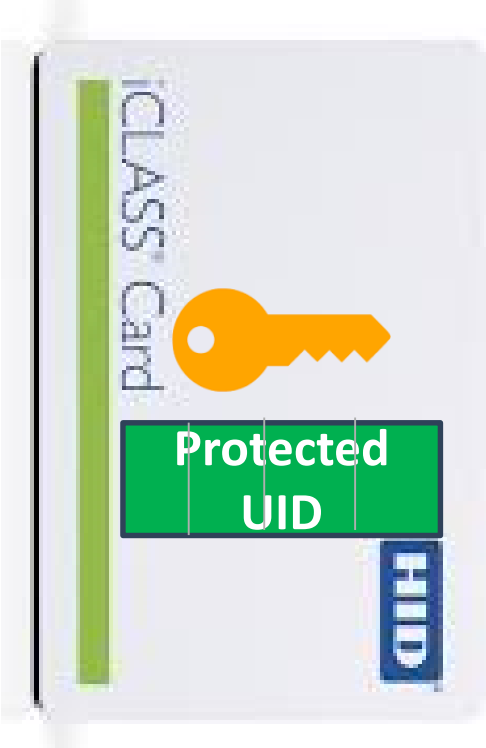
iClass security

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.*

https://www.hidglobal.com/doclib/files/resource_files/iclass_tag_ds_en.pdf

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.openpcd.org/images/HID-iCLASS-security.pdf

https://www.youtube.com/watch?v=mZNSYw9oH4Y

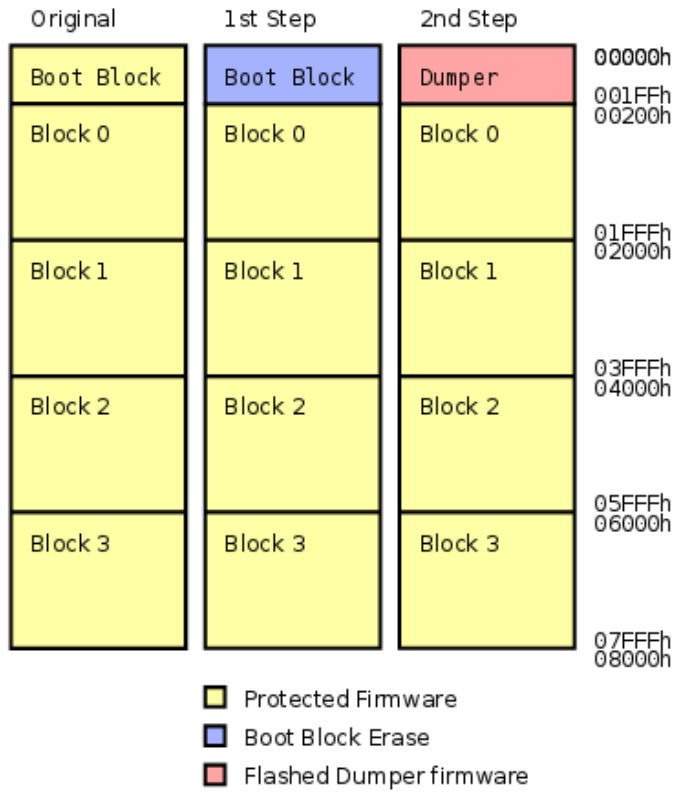


Fig. 6. In the first step EEPROM and FLASH content except of the boot block is dumped via UART.

The iClass leaked key

T0py
@InfoSecFriends

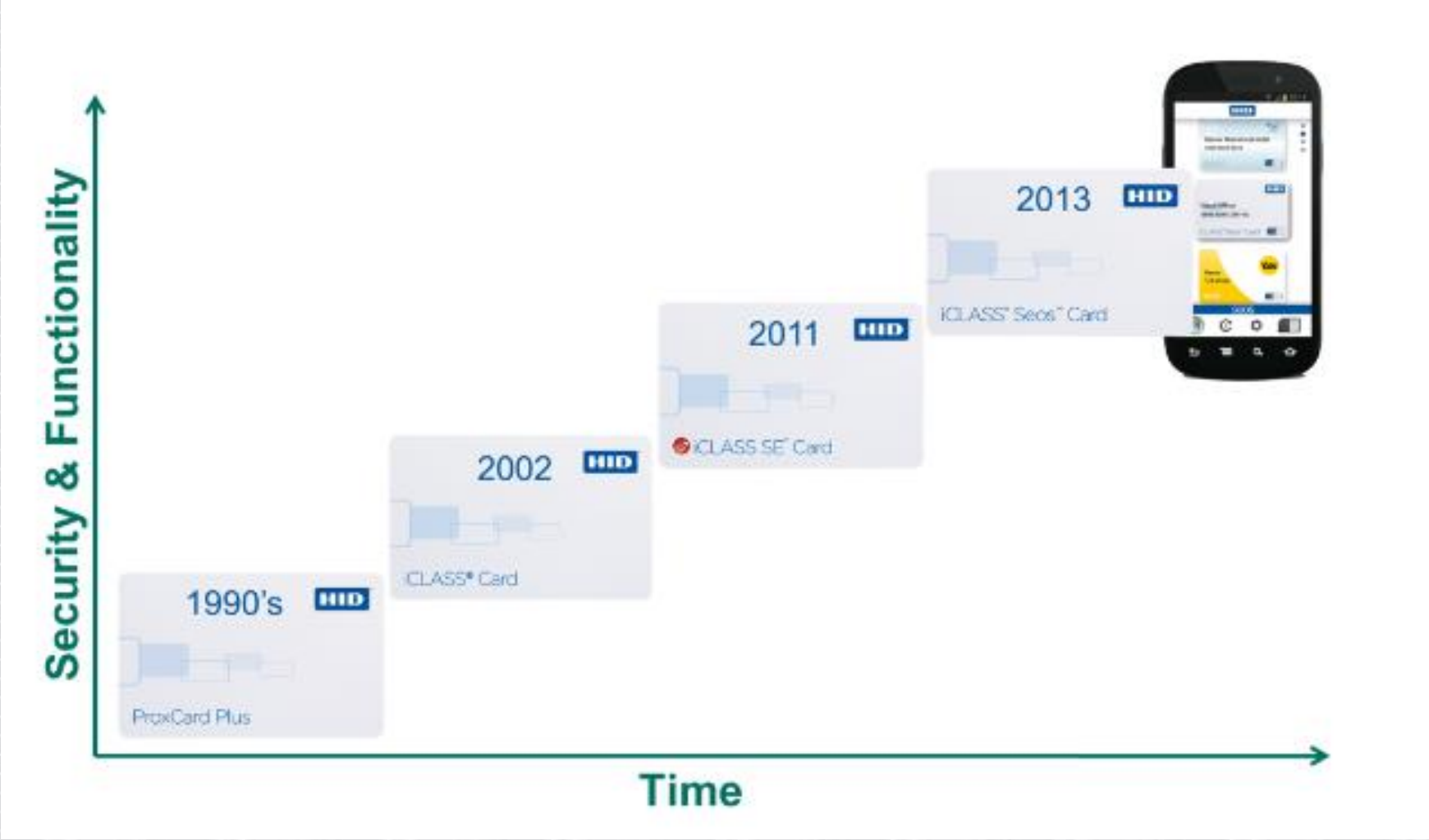
3F90EBF0910F7B6F
HID iClass Master key
Thanks @Amm0nRa <3
#kiwicon
#FuckCensorship

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



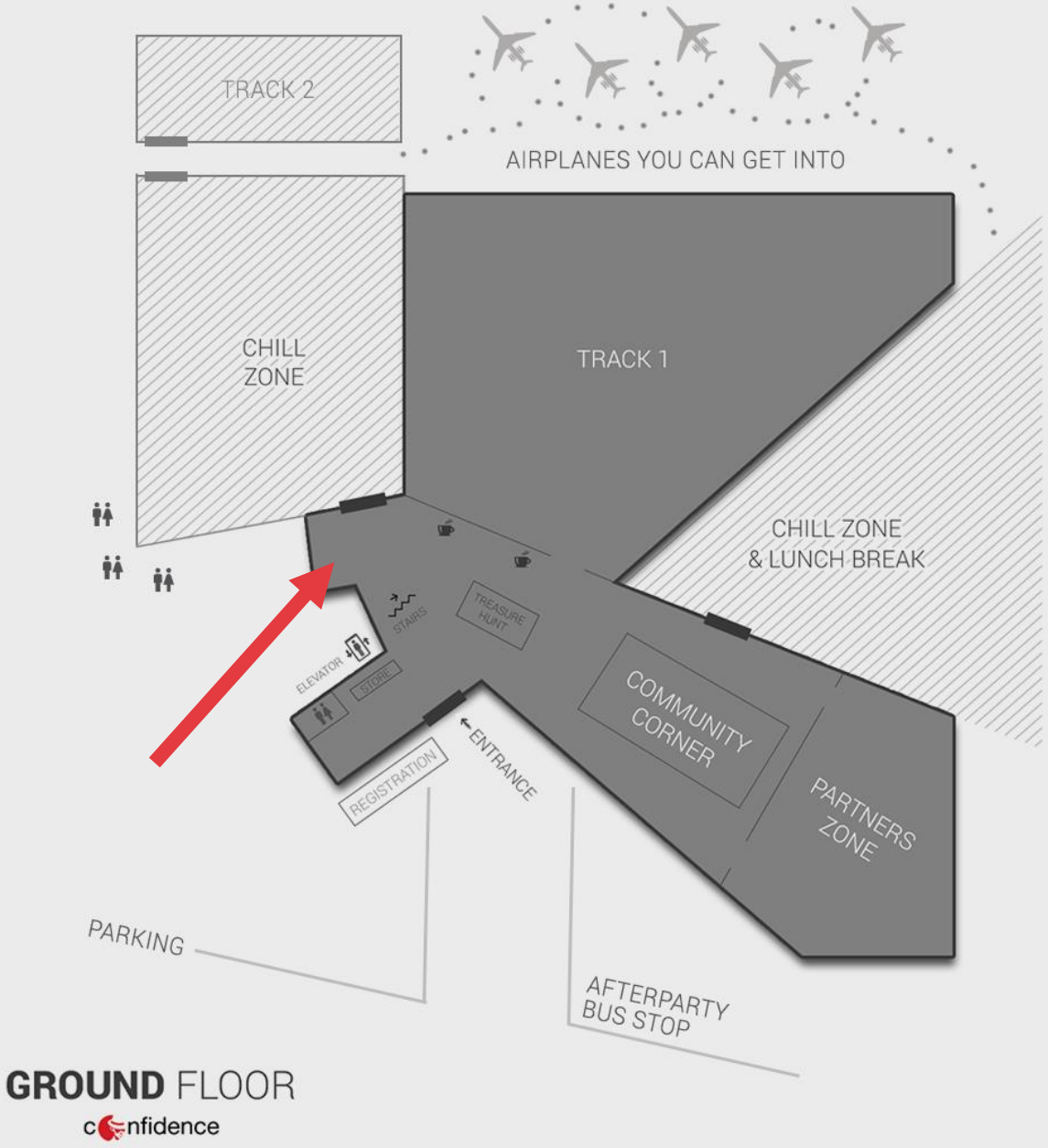
http://www.emacs.es/downloads/WP/20140723_iCLASS_Seos_Card_Whitepaper_EXTERNAL_v1.0.pdf

By the way...

Want to learn more about readout protection?

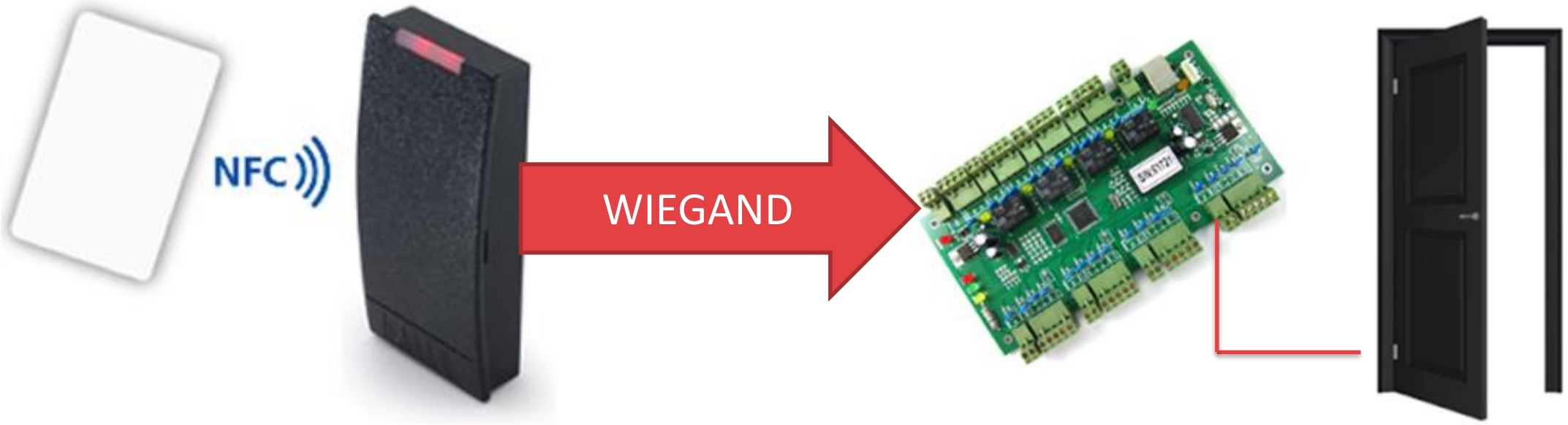
Come visit our booth (near chill zone), I will show you how to bypass it on STM32 (one of the most common IoT microcontrollers).

Today at 15.15, tomorrow at 12:35.

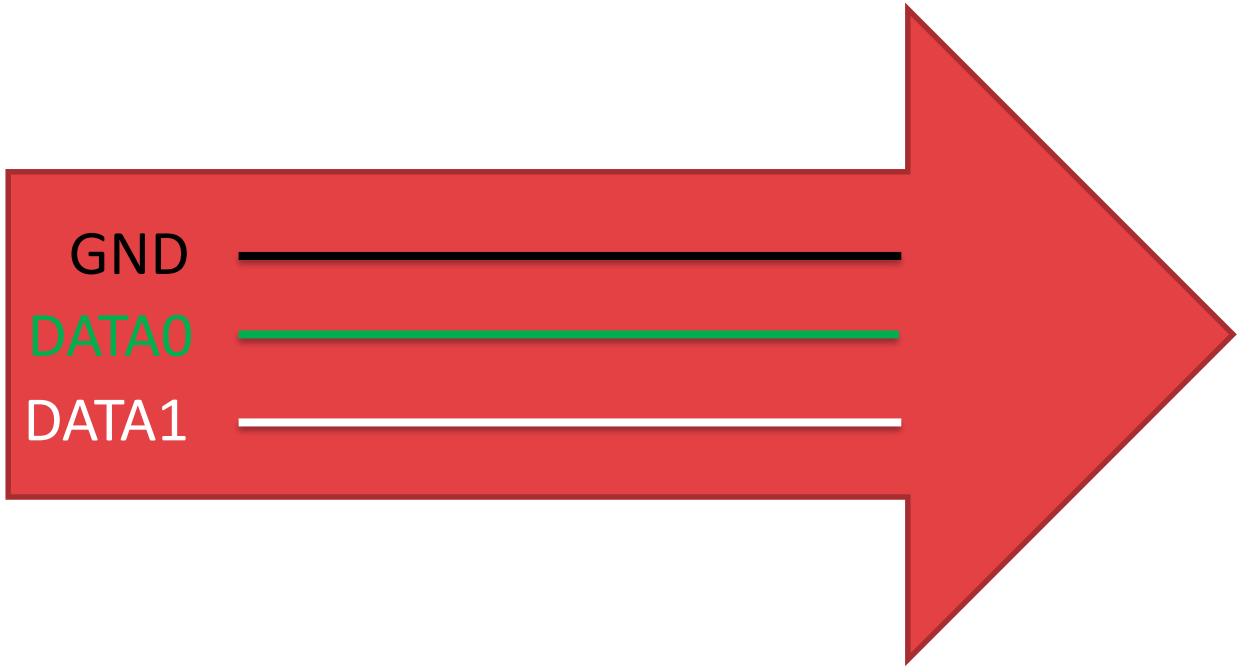


WIEGAND

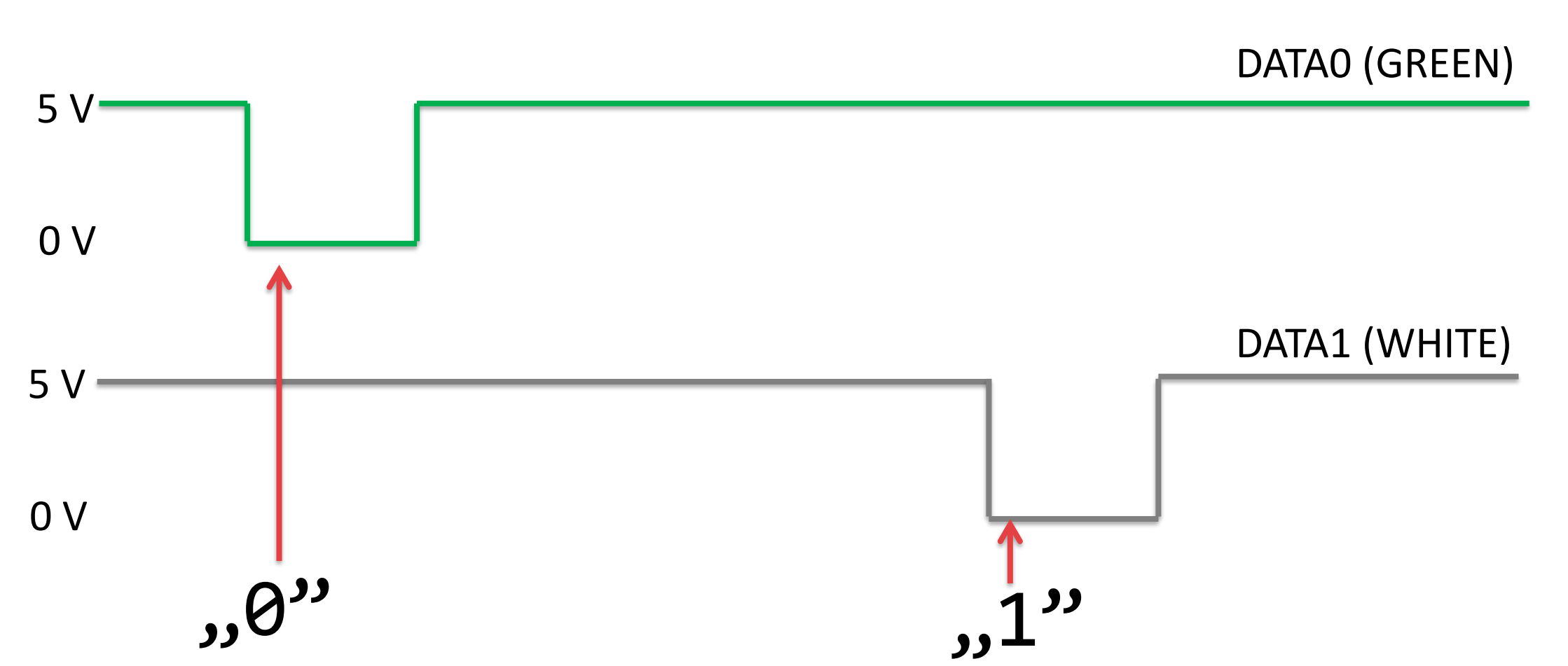
Typical architecture



3 wires – black, green, white



Transmitting 1's and 0's

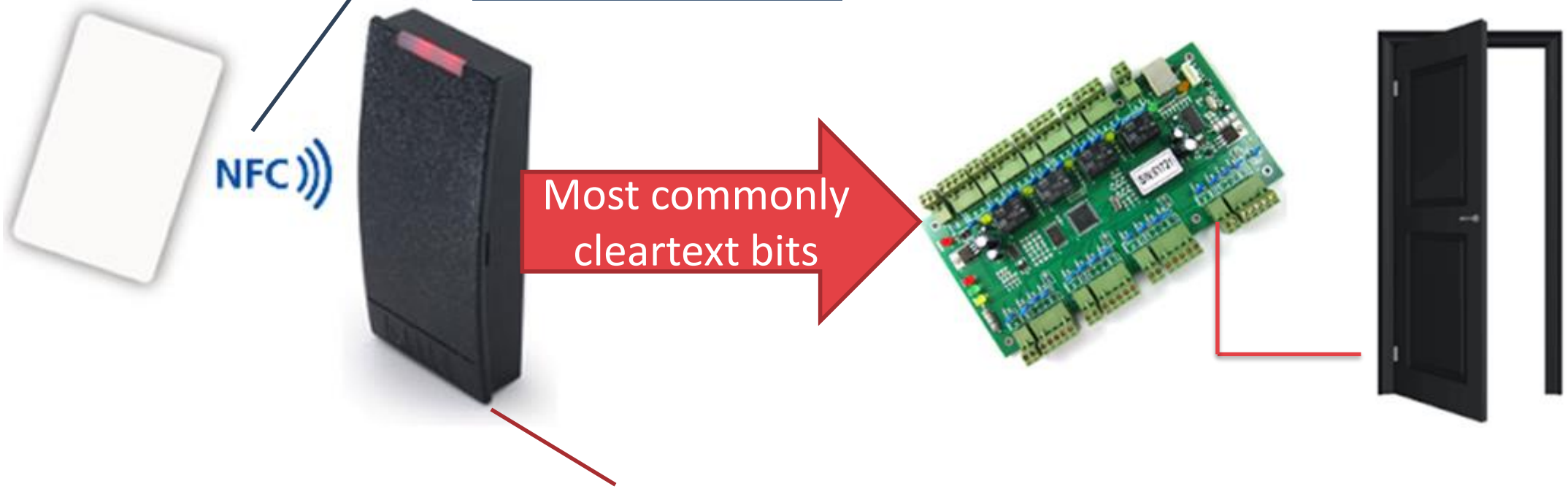


Card data transmitted: most common 26-bit

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

Typical architecture

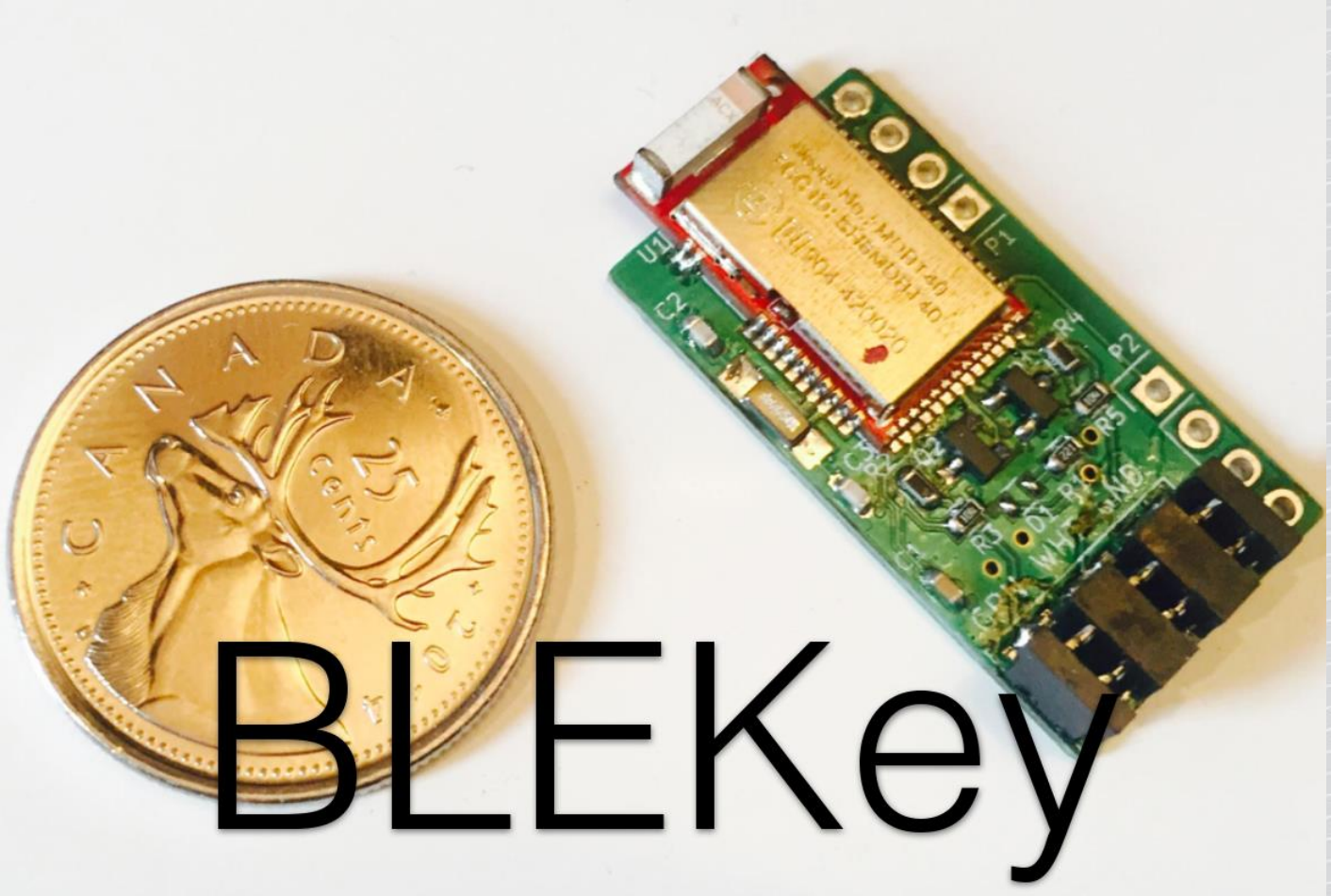
Sometimes secured, or hard to clone a card



Most commonly cleartext bits

External wall reader, quite often easy to detach

Wiegand sniffers: BLEKey



Install covertly in the reader, control from mobile app

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

Applications | Android Webcam Server... | Mozilla Firefox | [esprfidtool - File Manag... | 06:48:48 PM | root

Mozilla Firefox

http://192.168.1.169/

192.168.1.169

Most Visited | LegacySecurityGroup | exploitagency | Offensive Security

ESP-RFID-Tool v1.0.4

RFID TOOL

by Corey Harding
www.LegacySecurityGroup.com / www.Exploit.Agency

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

Android Webcam Server - Mozilla Firefox

Android Webcam Server

192.168.1.147:8080/browserfs.html

Most Visited | LegacySecurityGroup | exploitagency | Offensive Security

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

Best practices?

Tamper protection in readers.

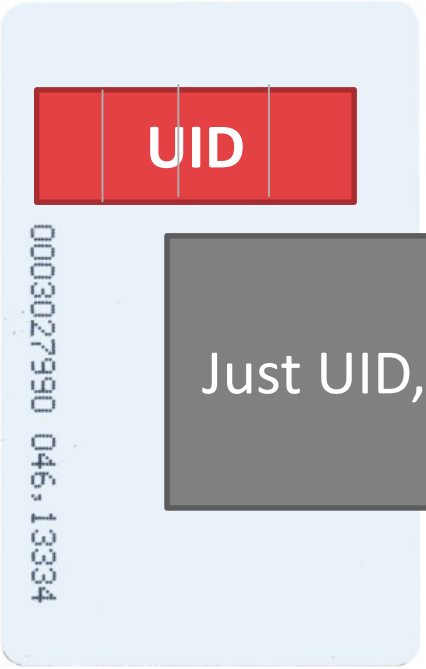
Multiple layers of security - intrusion detection, monitoring, behavioral analysis, ...

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

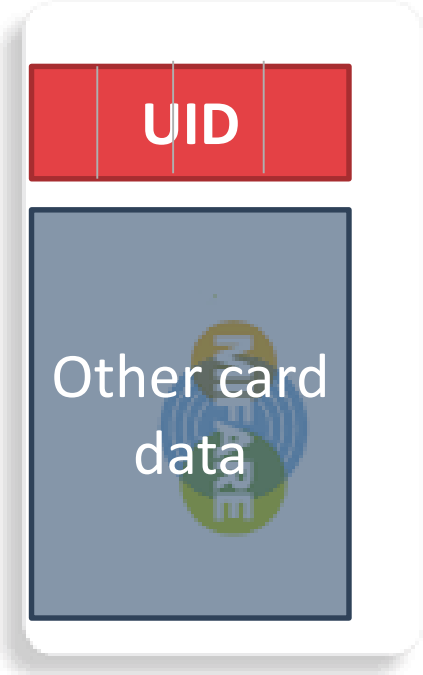


Just UID, no data

EM41XX („Unique”)

HID Prox II, Indala...

13.56MHz („high frequency”) NFC



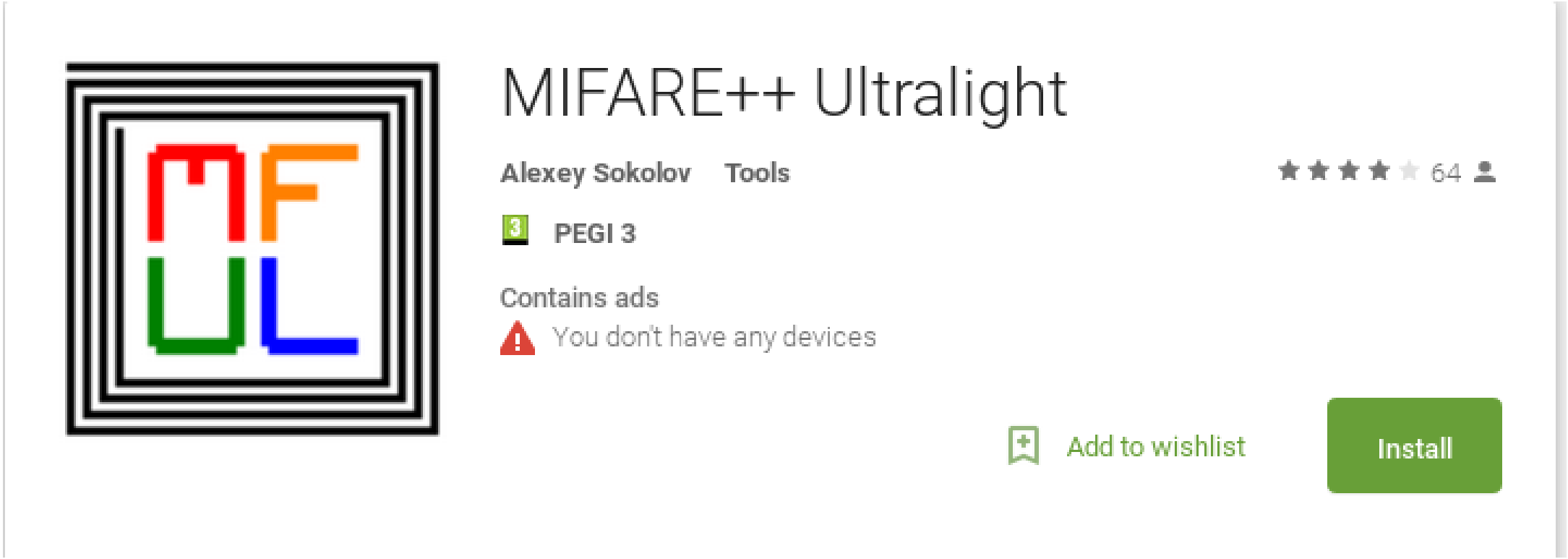
Mifare

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

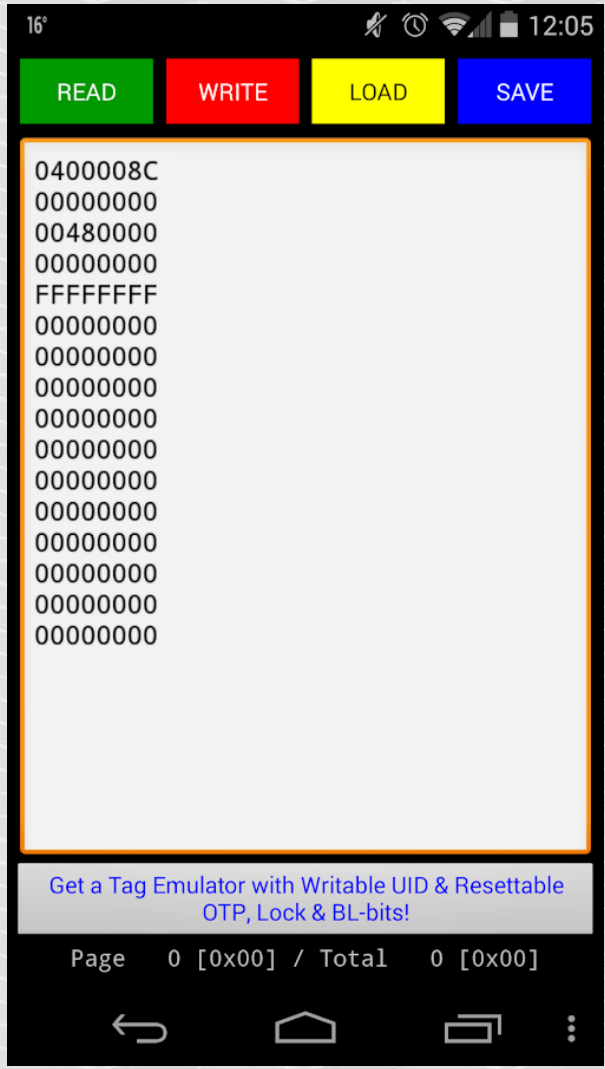


https://play.google.com/store/apps/details?id=com.samsung.sprc.fileselector

Android mobile application

Choose „READ” and place the tag

Scanned content

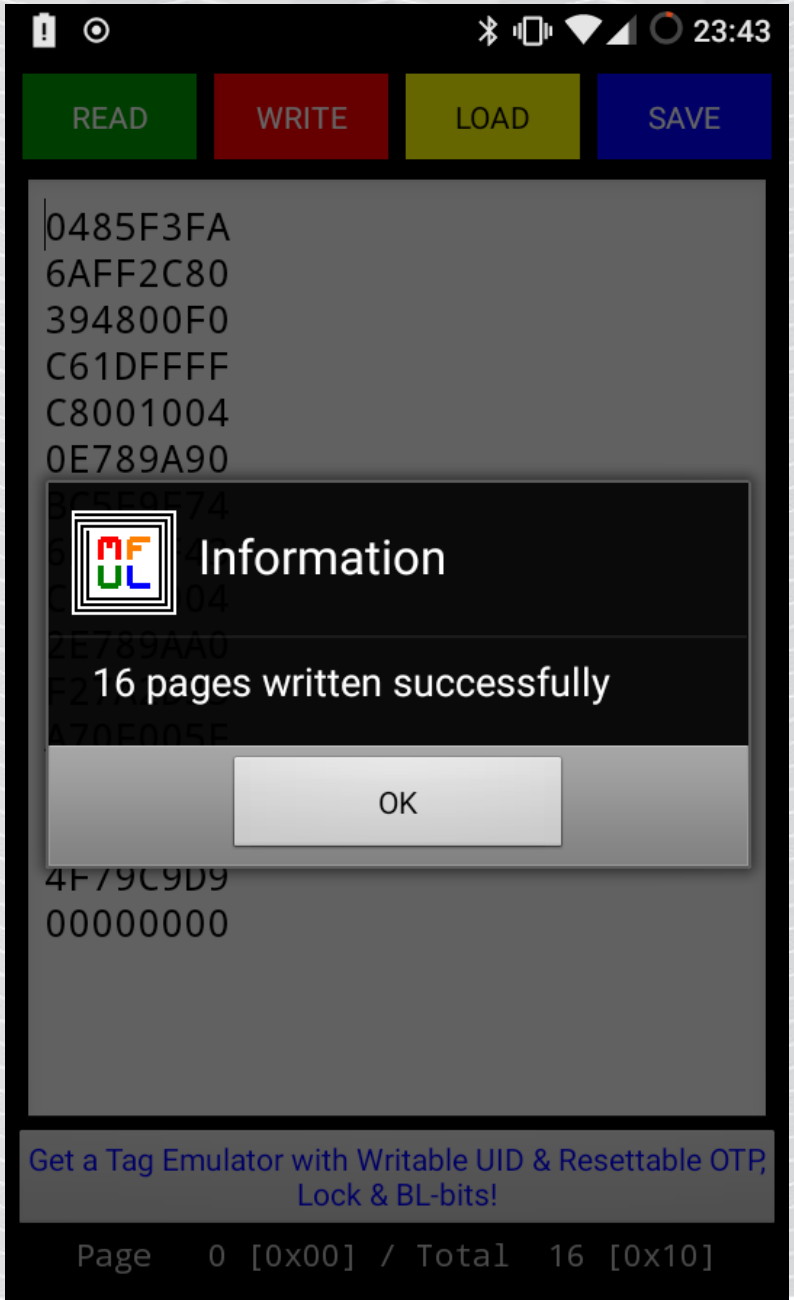


Android mobile app - write

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

Mifare Classic

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.*

https://www.mifare.net/wp-content/uploads/2015/03/MIFARE_Classic_EV1.pdf

City cards, access control, student id, memberships, internal payment, tourist card, ski pass, hotels, ...

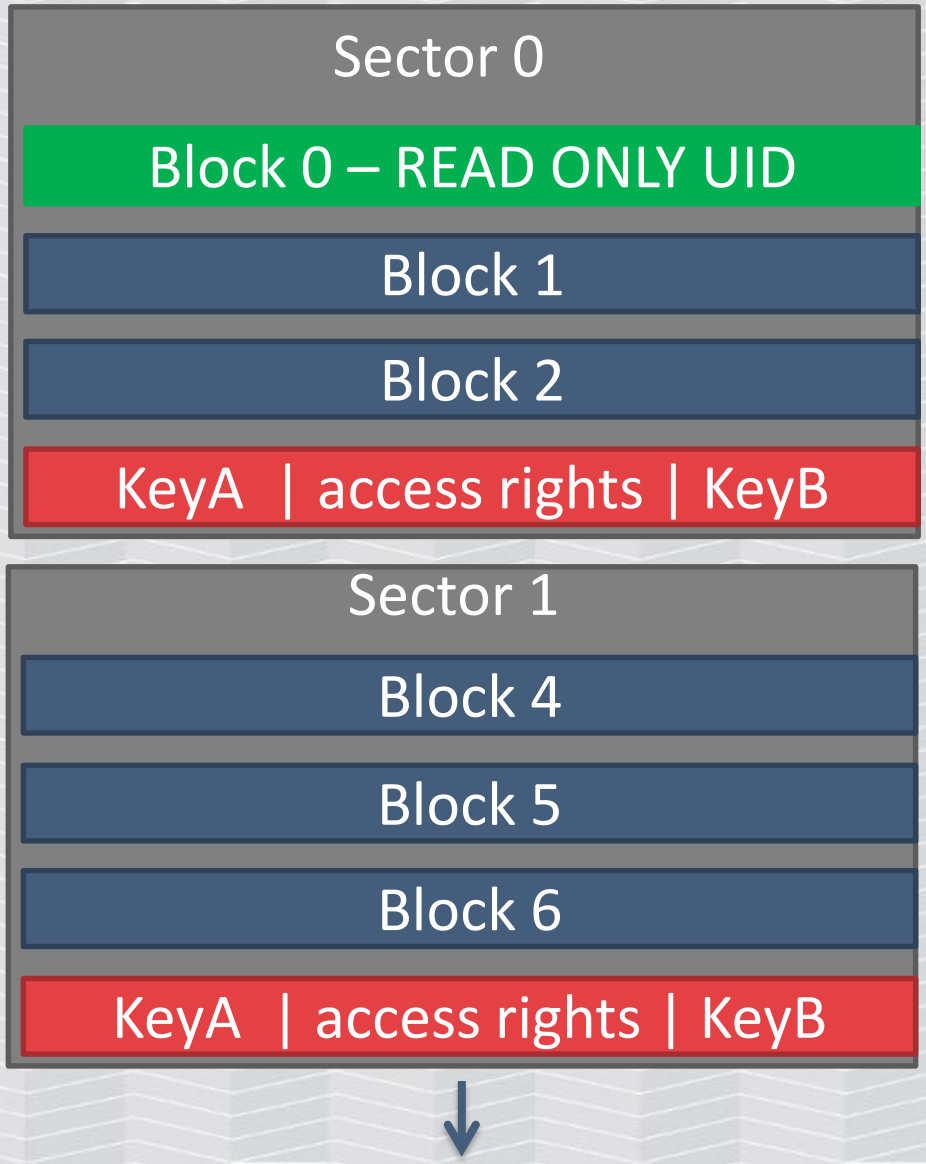
It’s everywhere…

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

FFFFFFFFFFFF (default key)

A0A1A2A3A4A5

D3F7D3F7D3F7

000000000000

...

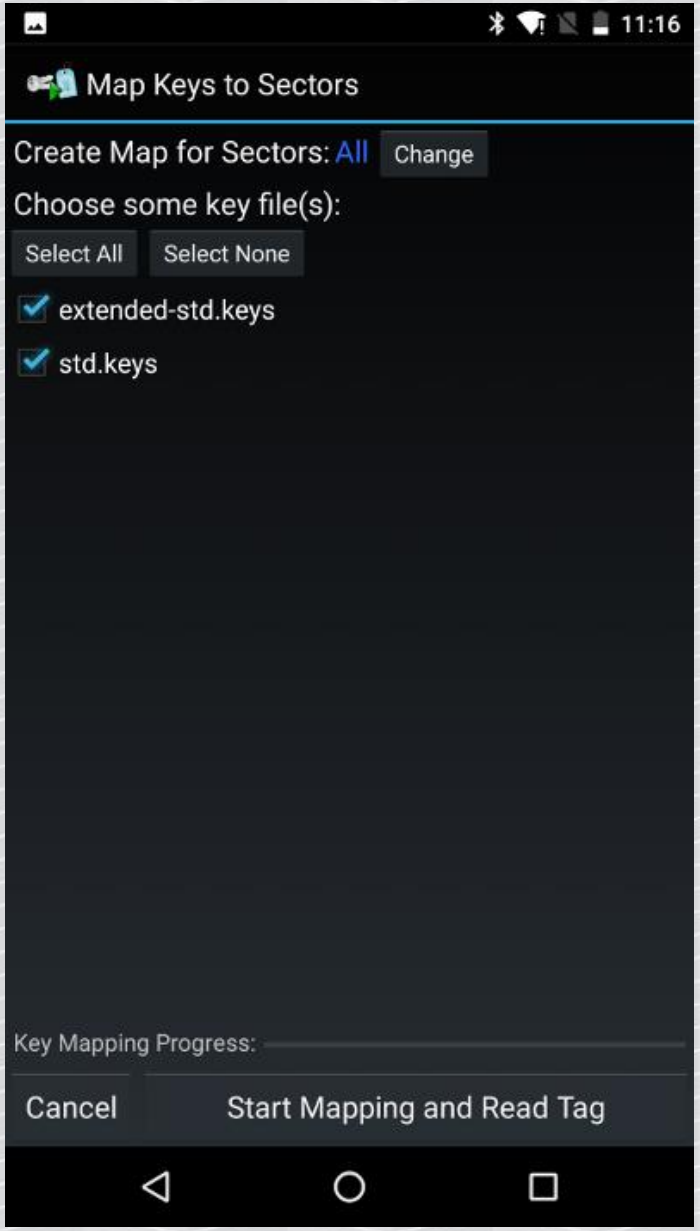
Using Android mobile app?

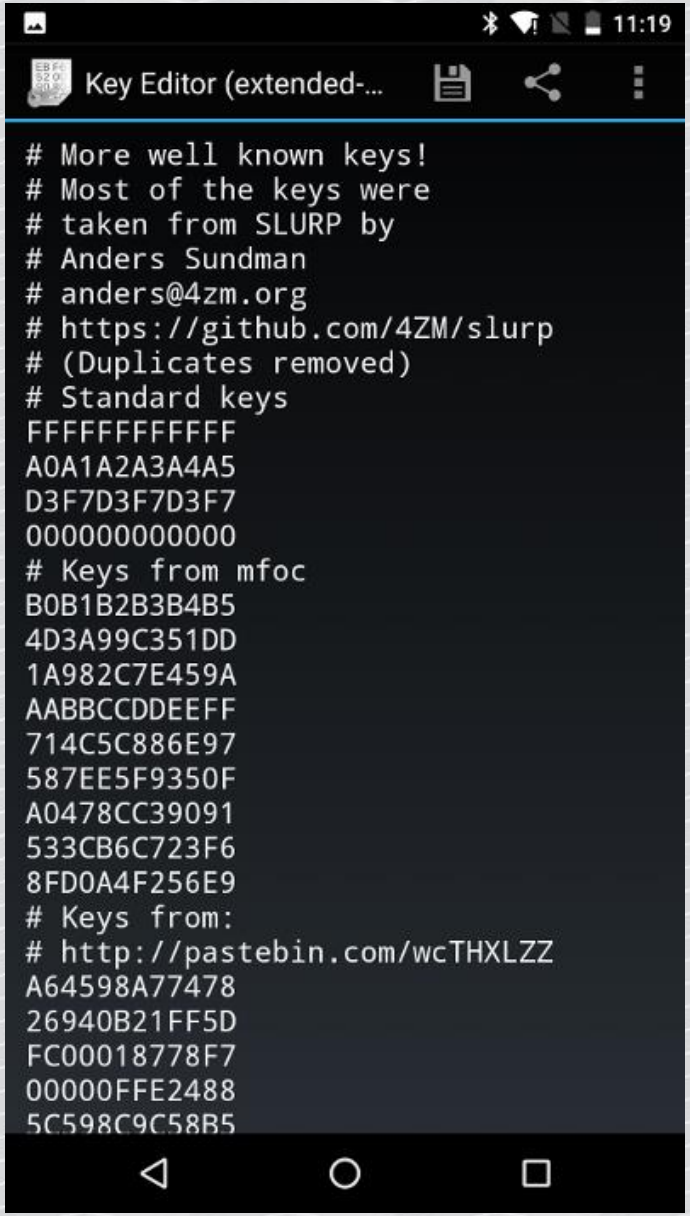
Mifare Classic Tool – free, opensource

Note: you need NXP NFC chipset (most current phones)

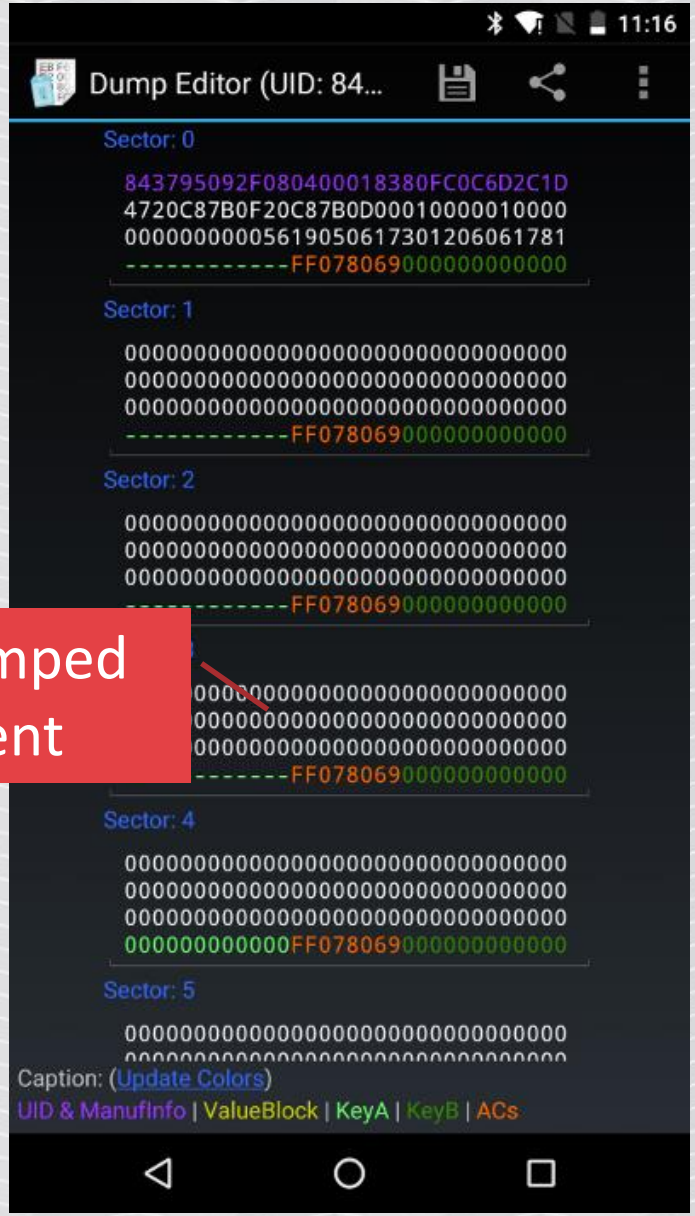
https://github.com/ikarus23/MifareClassicTool

https://play.google.com/store/apps/details?id=de.syss.MifareClassicTool

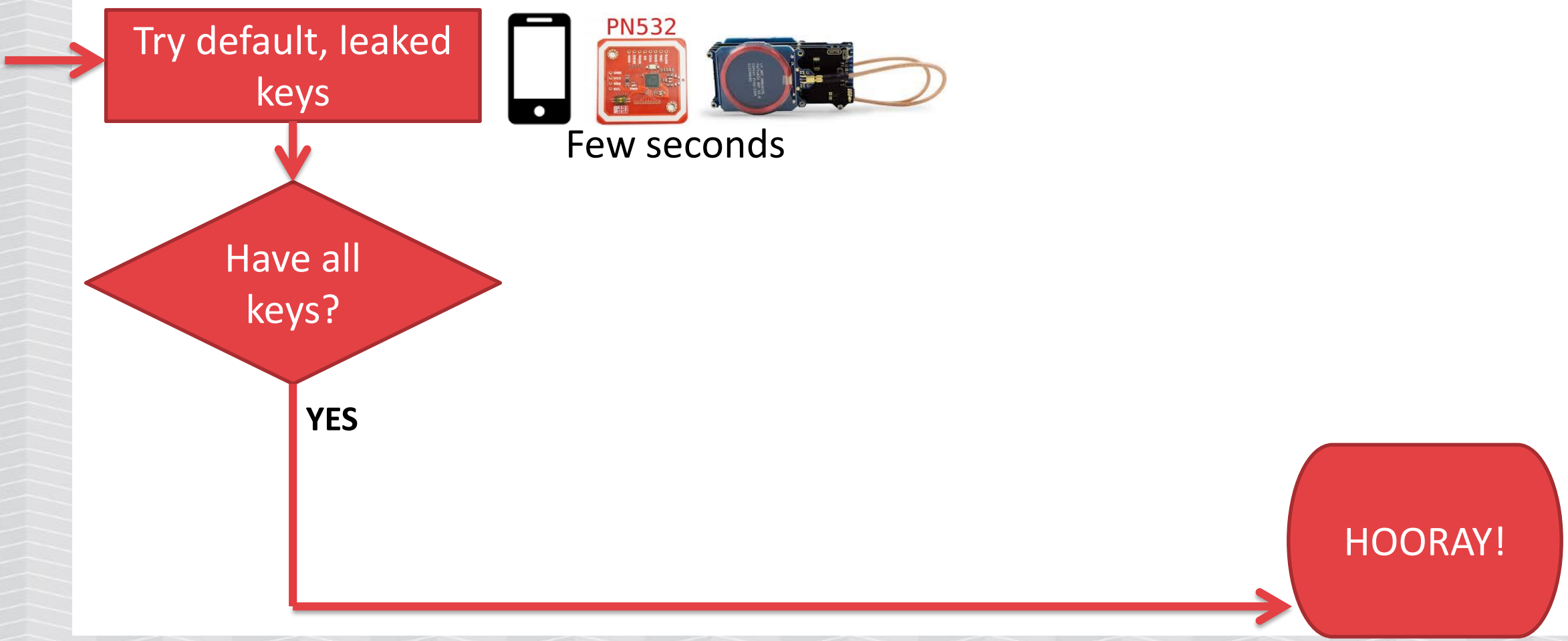




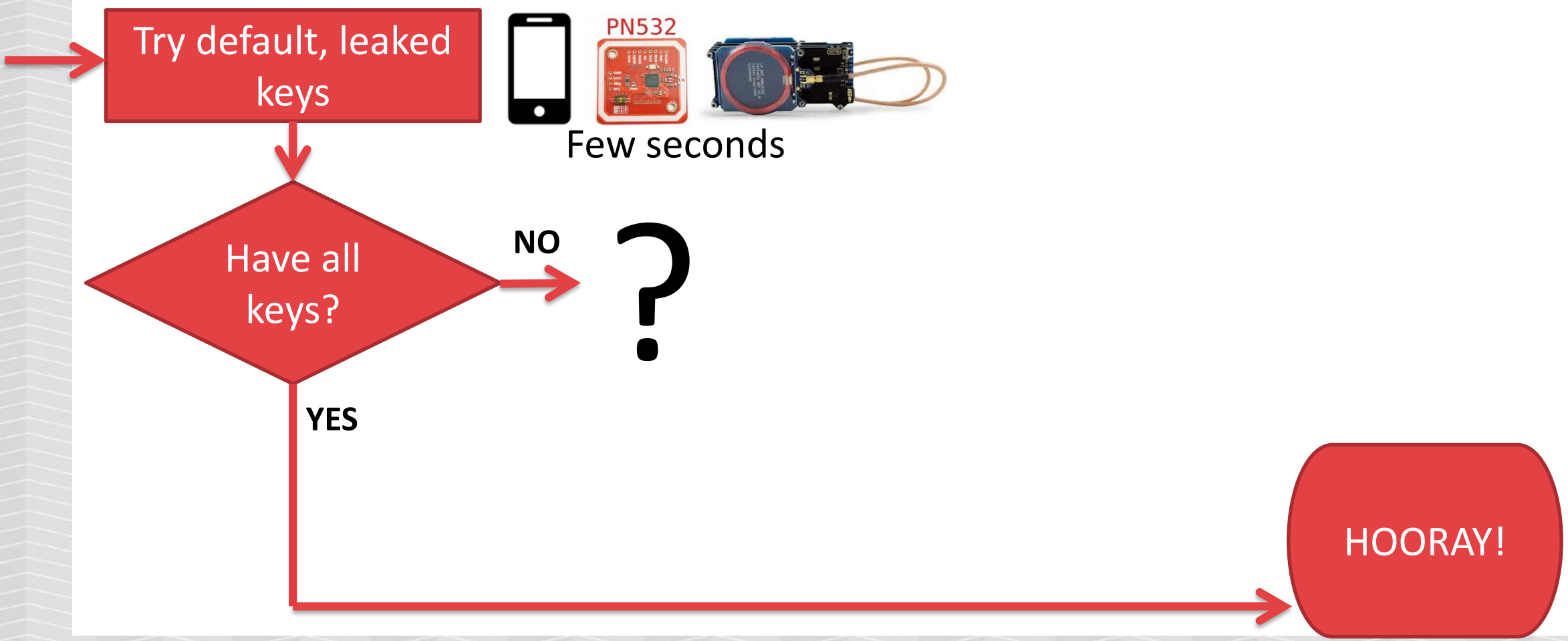
The dumped content



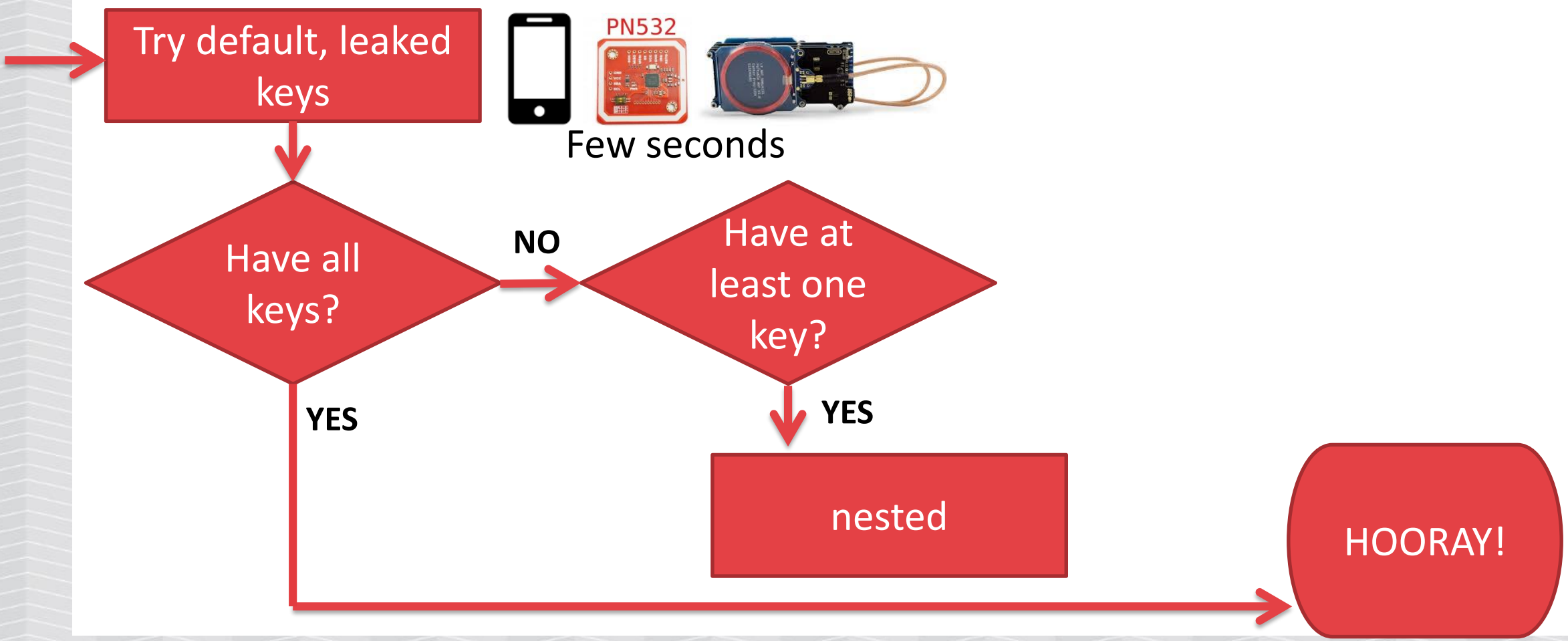
Mifare Classic cracking process



Mifare Classic cracking process



Mifare Classic cracking process



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):

http://www.cs.ru.nl/~flaviog/publications/Pickpocketing.Mifare.pdf

Sector 0
Key: FFFFFFFF

Sector 1
Key: unknown

Sector 2
Key: unknown

Sector 3
Key: unknown

Sector 4
Key: unknown

...

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 sector 00 as an exploit sector
Sector: 0, type A, probe 0, distance 12575 .....
Sector: 0, type A, probe 1, distance 12573 .....
Sector: 0, type A, probe 2, distance 12571 .....
Sector: 0, type A, probe 3, distance 12567 .....
  Found Key: A [                    ]
```

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

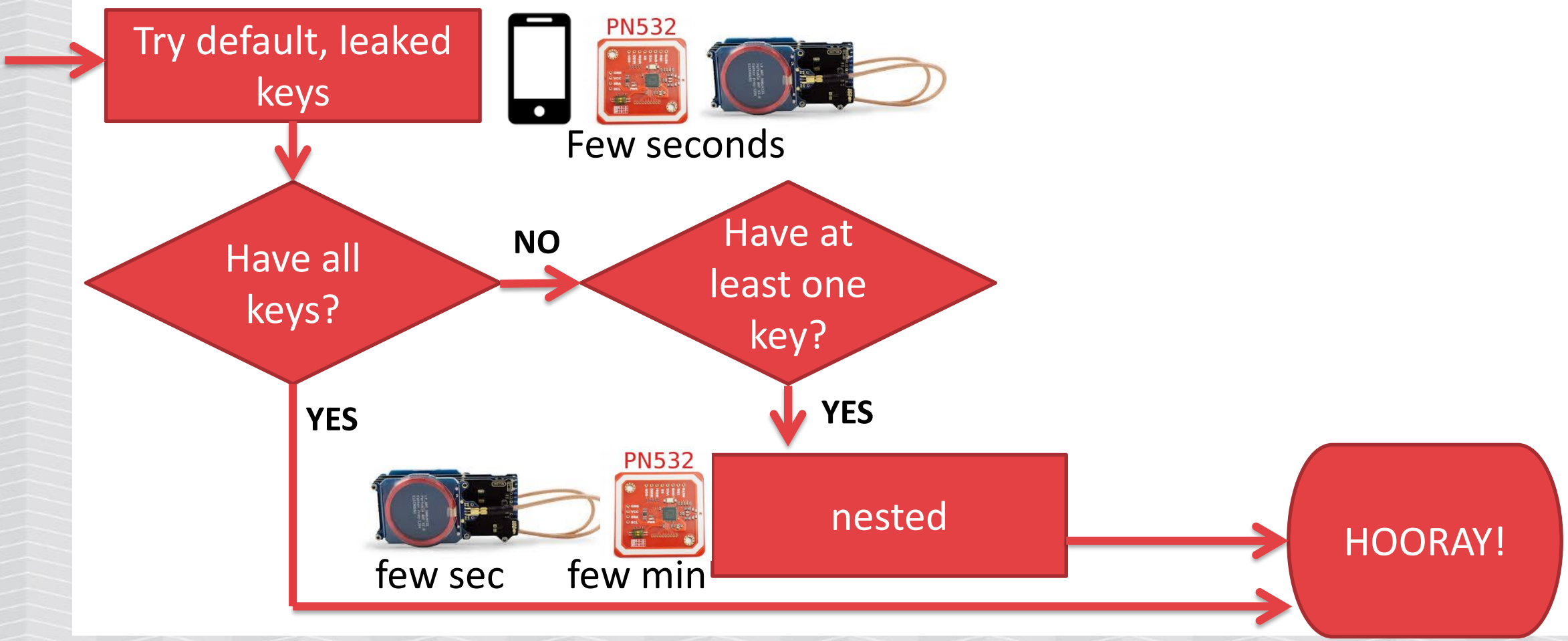
US $4.18 / Set

Using proxmark?

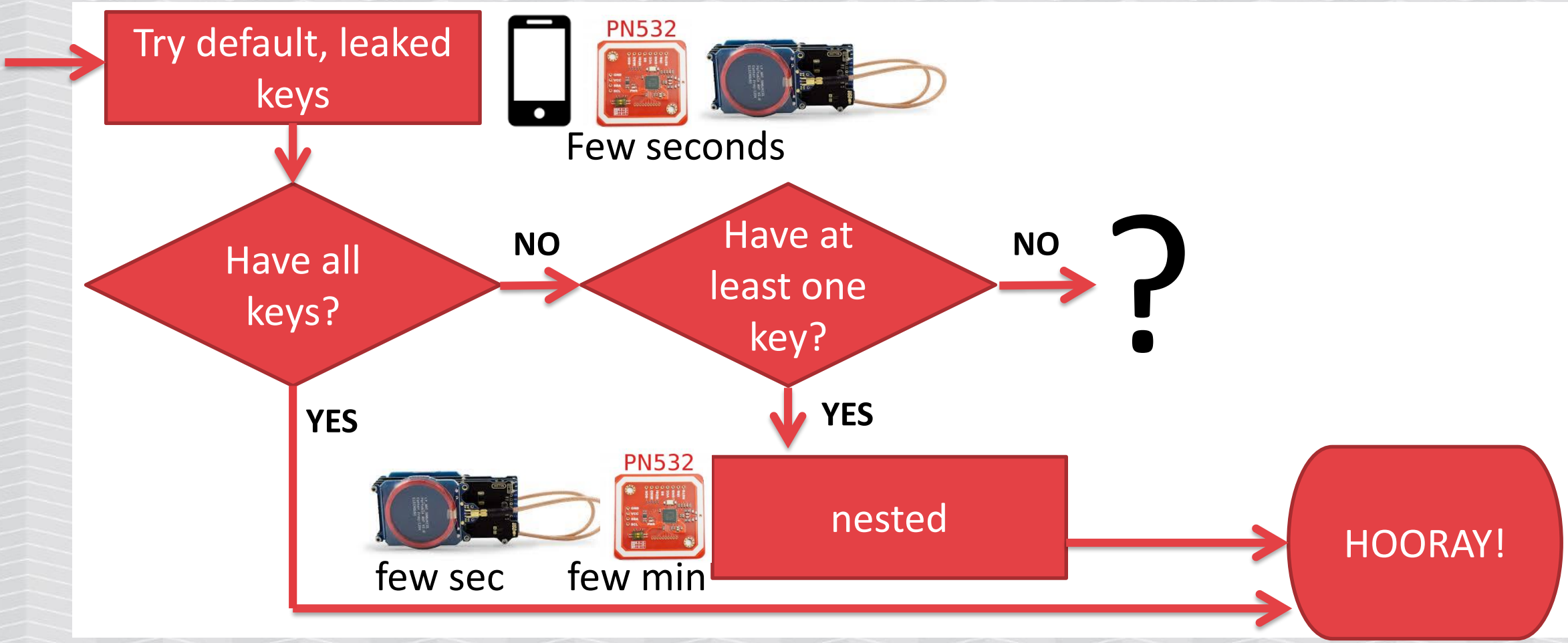
```
pm3 --> hf mf nested 1 0 B ffffffffffff d
Testing known keys. Sector count=16
[-] Chunk: 0,8s | found 29/32 keys (21)

[+]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



Mifare Classic cracking process



But what if all the keys are unknown?

„Darkside" attack, Nicolas T. Courtois – side channel. Tech details (2009):

https://eprint.iacr.org/2009/137.pdf

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".

Sector 0
Key: unknown

Sector 1
Key: unknown

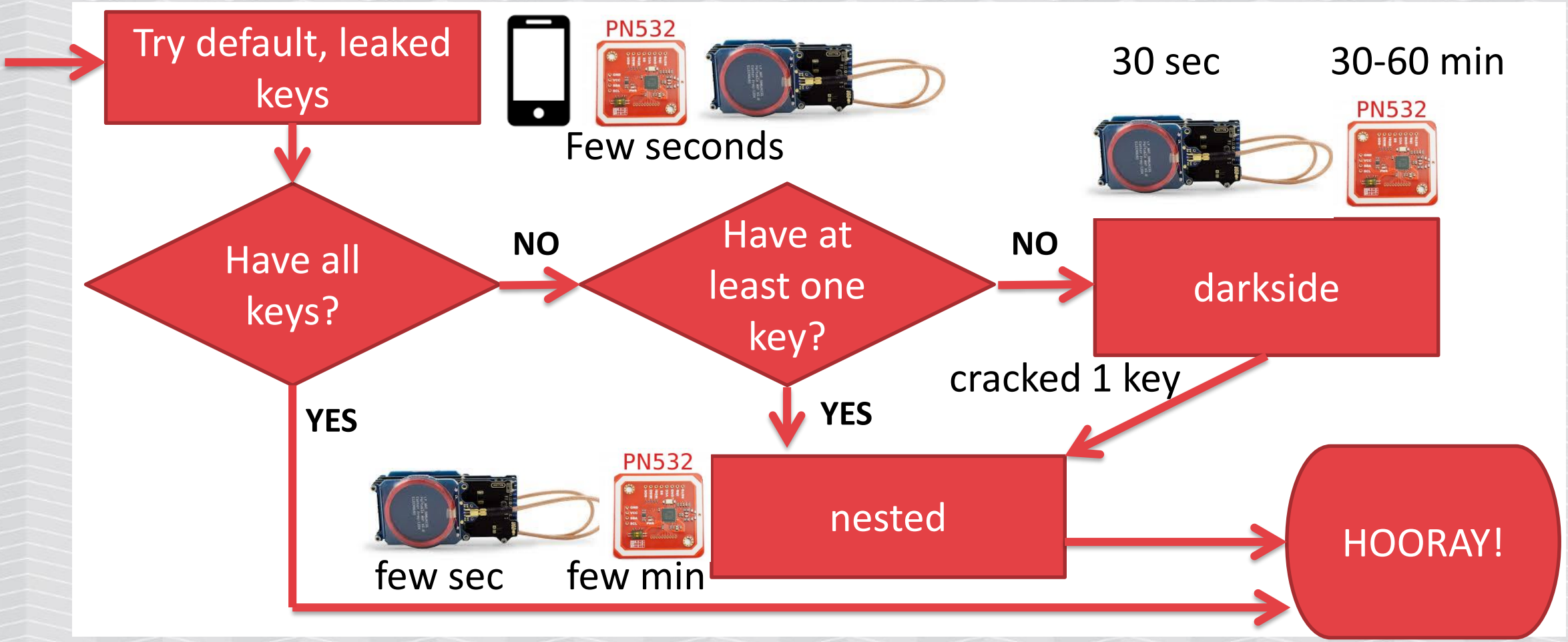
Sector 2
Key: unknown

Sector 3
Key: unknown

Sector 4
Key: unknown

...

Mifare Classic cracking process



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

„Hardnested" attack – exploits CRYPTO1 weakness. Tech details (2015):

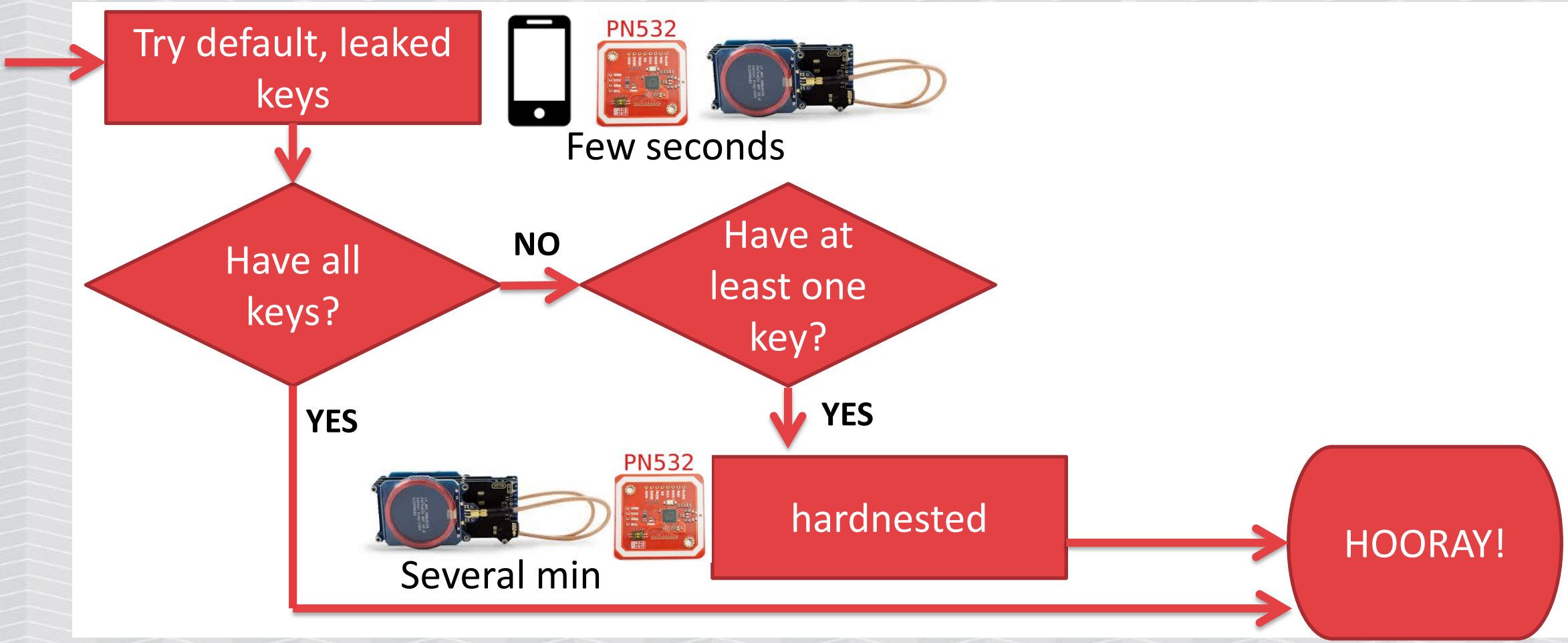
http://cs.ru.nl/~rverdult/Ciphertext-only_Cryptanalysis_on_Hardened_Mifare_Classic_Cards-CCS_2015.pdf

PN532 libnfc: miLazyCracker - automatically detects card type, proceeds with relevant attack scenario:

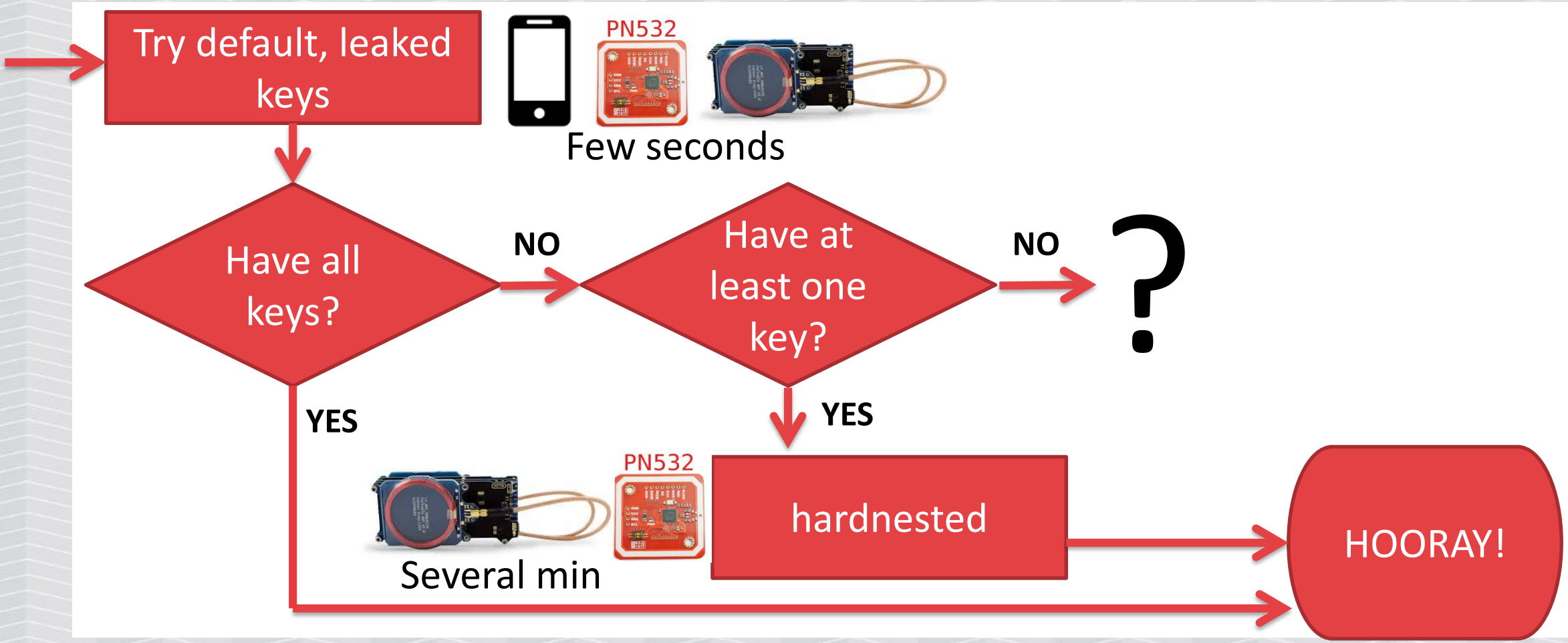
https://github.com/nfc-tools/miLazyCracker

https://www.youtube.com/watch?v=VcU3Yf5AqQI

Mifare Classic hardened (Plus SL1, EV1) cracking



Mifare Classic hardened (Plus SL1, EV1) cracking



EV1 with all sectors secured?

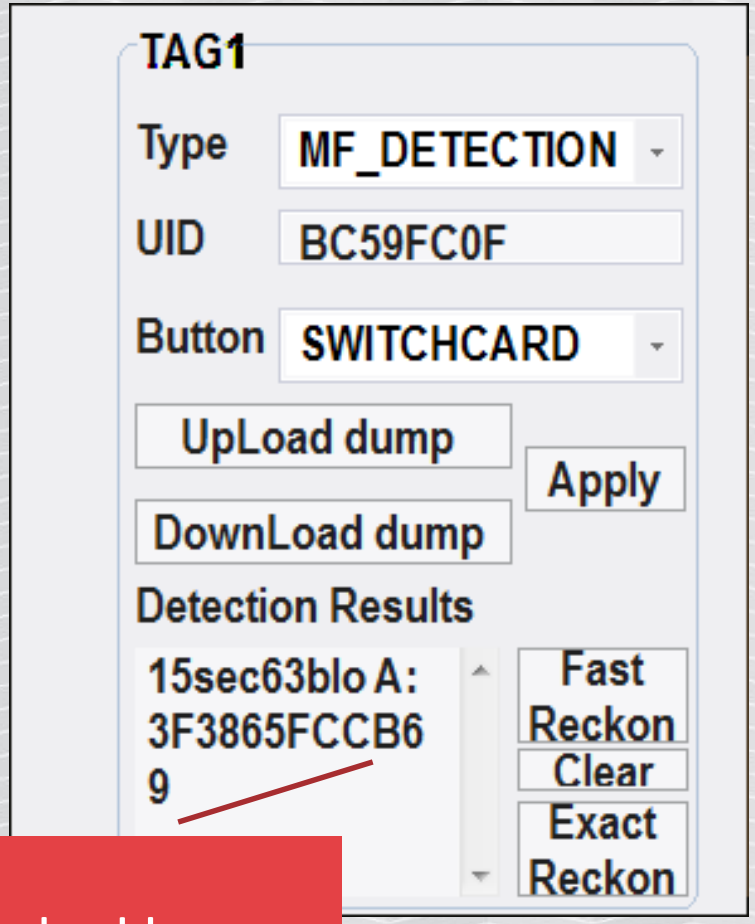
„Hardnested" requires at least one known key. Wha
if all the keys are unknown?

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

Hardware: Proxmark, Chameleon Mini RevE
„Rebooted"

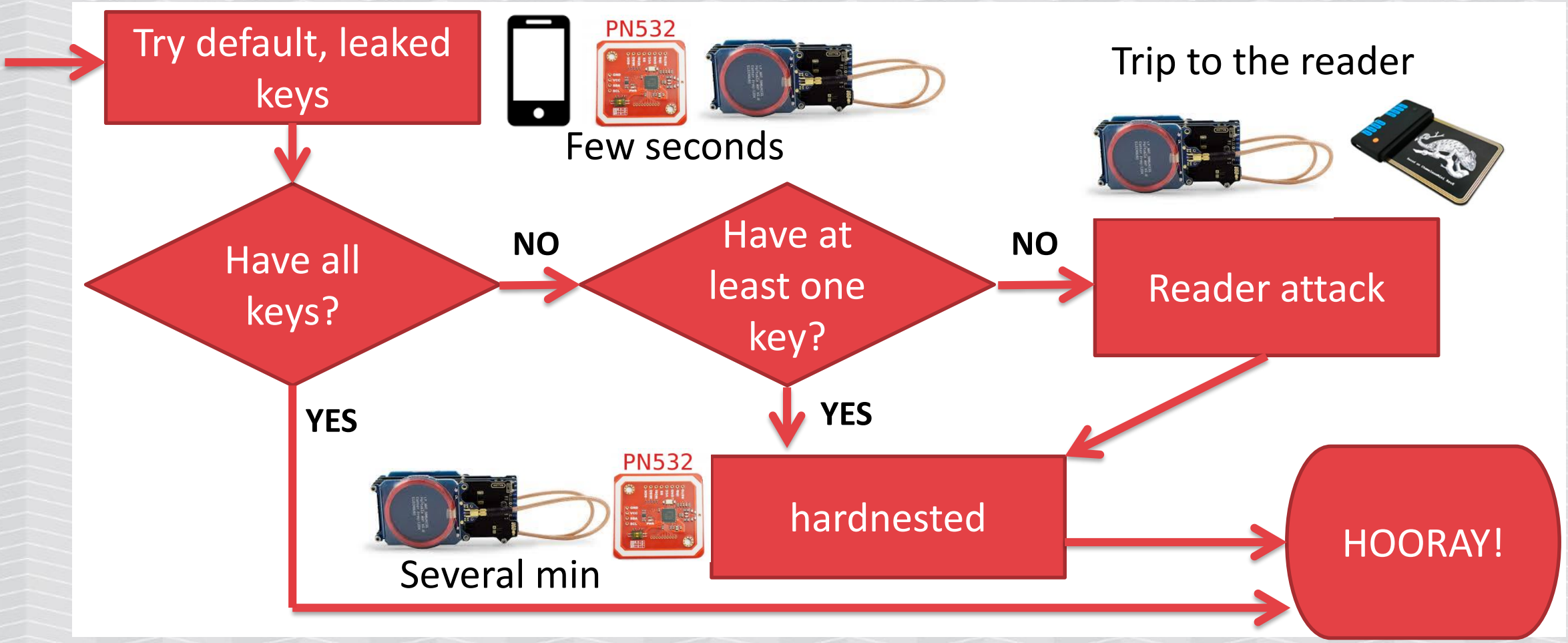
Chameleon Mini reader attack

1. Set MF_DETECTION
2. Place the Chameleon at reader
3. Download dump
4. „Reckon" (mfkey) – cracks the key



Cracked key

Mifare Classic hardened (Plus SL1, EV1) cracking



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.

https://www.mifare.net/en/products/chip-card-ics/mifare-classic/security-statement-on-crypto1-implementations/

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.

```
047D4CBD
0AAE5980
7D480800
3C040D0D
060A0021
00000000
0000F969
B871144B
1B2460BD
F9F9F9F0
4290FC39
06F9F97B
F9F9F9F9
F9F9F9F9
F9F9F922
E7AA8783
```

Hotel: 2 cards for the same room

Card UID

Encoded access data?

Checksum?

```
04 25 69 C0 42 DD 29 80  36 48 00 00 09 01 65 0D
06 0A 00 21 00 00 [illegible] E EE 5F 71 06 FC
[illegible] F9 7D 7E C6 7D E2 60 7E BE 81 7E FF 7E
42 7E 7E 7E 7E 7E 7E 7E  7E 7E 7E 00 58 94 D8 A9
```

```
04 95 68 71 42 DD 29 80  36 48 00 00 18 [illegible]
06 0A 00 21 00 00 00 00  00 00 82 12 A3 8D FA C0
2B 8B 55 05 81 82 3A 81  1E 9C 82 42 7D 82 03 82
BE 82 82 82 82 82 82 82  82 82 82 00 68 99 E8 A0
```

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

The encoded data

Card 1

```
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
```

Card 2

```
82 12 A3 8D FA C0 2B 8B 55 05 81 82 3A 81 1E 9C 82
42 7D 82 03 82 BE 82 82 82 82 82 82 82 82 82 82
```

The encoded data

Card 1

```
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
```

Repeating 7E

Card 2

```
82 12 A3 8D FA C0 2B 8B 55 05 81 82 3A 81 1E 9C 82
42 7D 82 03 82 BE 82 82 82 82 82 82 82 82 82 82
```

Repeating 82

Maybe there were 00's in cleartext?

```
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
```

XOR

```
7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E (...)
```

=

```
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
```

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 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
```

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
```

Now just a few bytes differ

```
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
```

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

https://www.f-secure.com/en/web/business_global/electronic-lock-systems-are-vulnerable

Collect various hotel cards...

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

https://twitter.com/mikko/status/989154230723334151

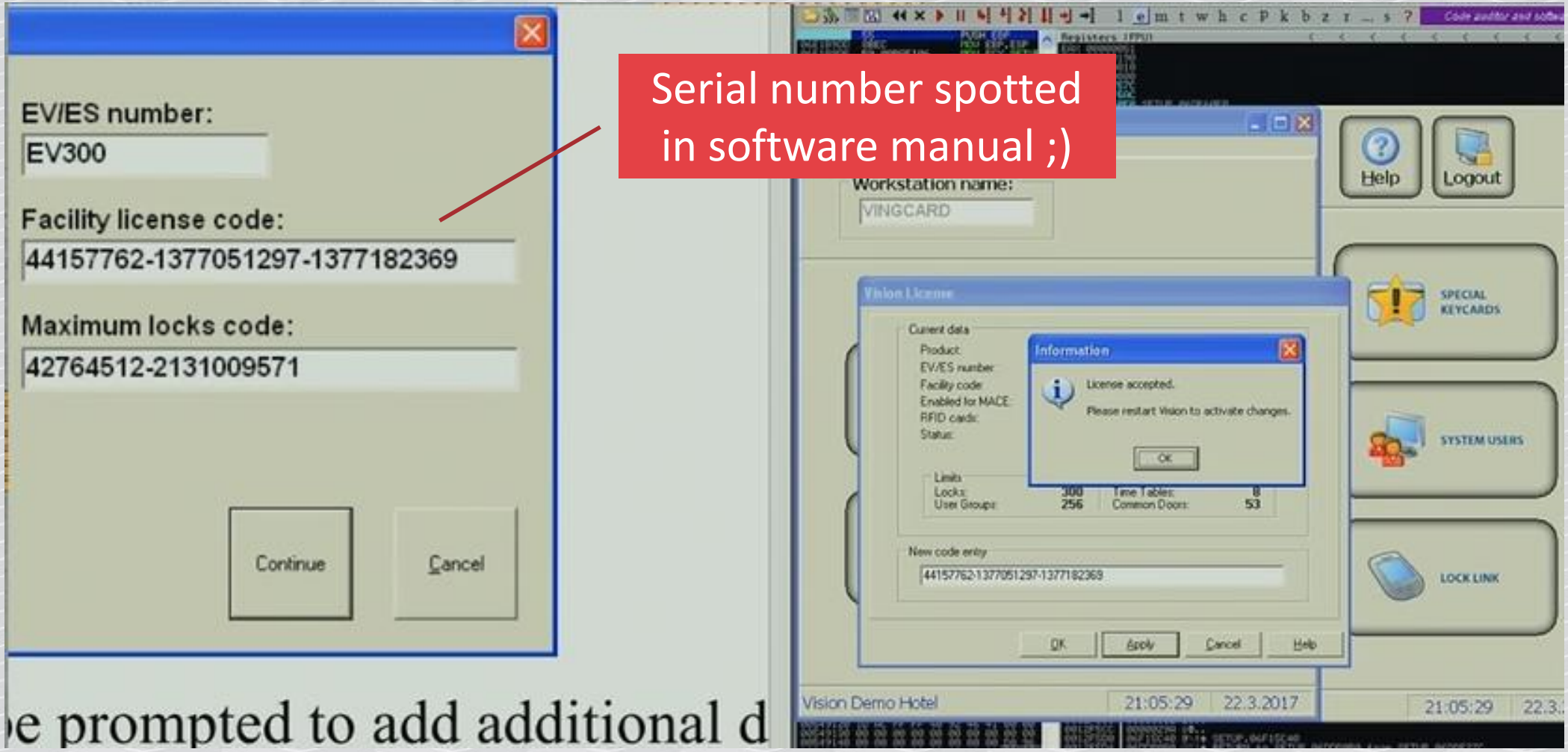
Get the hotel software

Index of /webdownloads/Vision_

Name	Last modified	Size	Description
Parent Directory		-	
Vision 6.3 Total CD .zip	27-May-2014 13:56	186M	
Vision Release Note V6.3.pdf	27-May-2014 13:57	483K	

Ghost in the locks, Tomi Tuominen, Timo Hirvonen, INFILTRATE 2018, https://vimeo.com/267613809

And its license…



Ghost in the locks, Tomi Tuominen, Timo Hirvonen, INFILTRATE 2018, https://vimeo.com/267613809

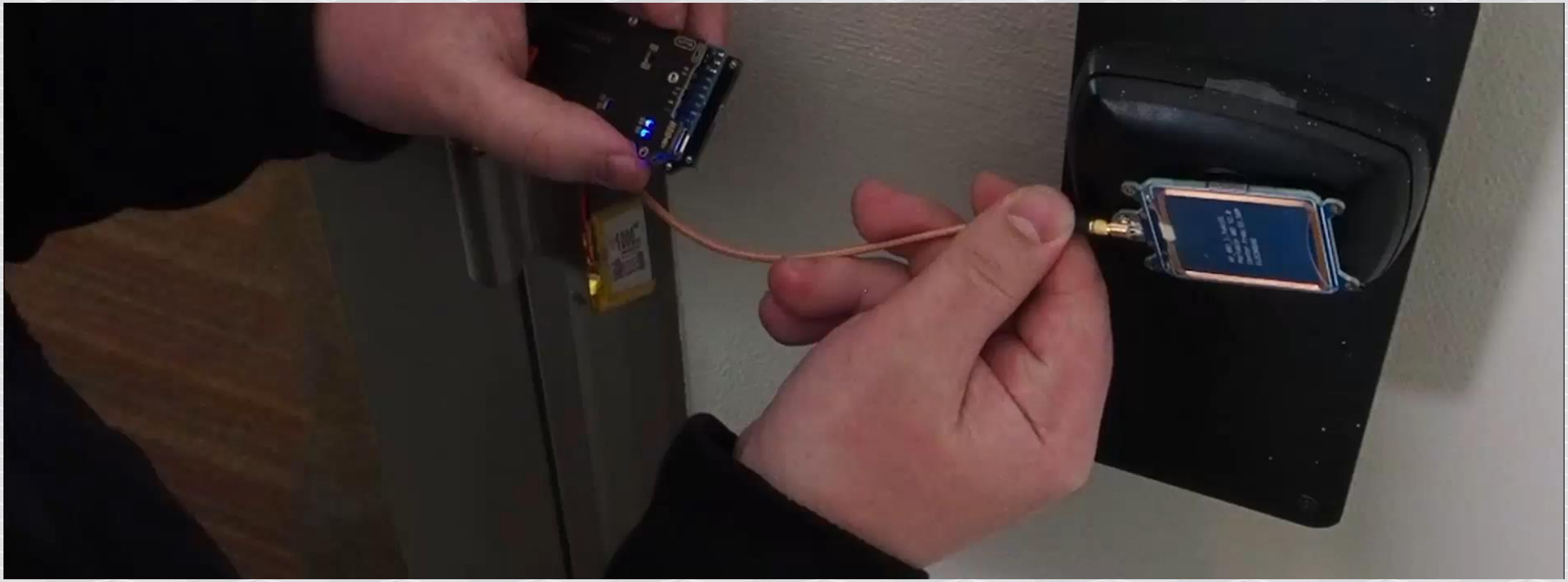
The „master” card

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



https://www.f-secure.com/documents/10192/2302132/ghost-in-the-lock.mp4

Other hotel system: guest card data

I checked in yesterday evening.

```
47 00 00 48 3B 00 93 4F B1 00 00 00 01 14 00 00
00 00 00 00 01 47 20 03 06 18 00 15 13 06 18 8D
```

Can you tell me the check out date and time?

How about the room number?

Hotel guest card data

Room number: 114

```
47 00 00 48 3B 00 93 4F B1 00 00 00 01 14 00 00
00 00 00 00 01 47 20 03 06 18 00 15 13 06 18 8D
```

Check in: 2018.06.03 20:47

Check out: 2018.06.13 15:00

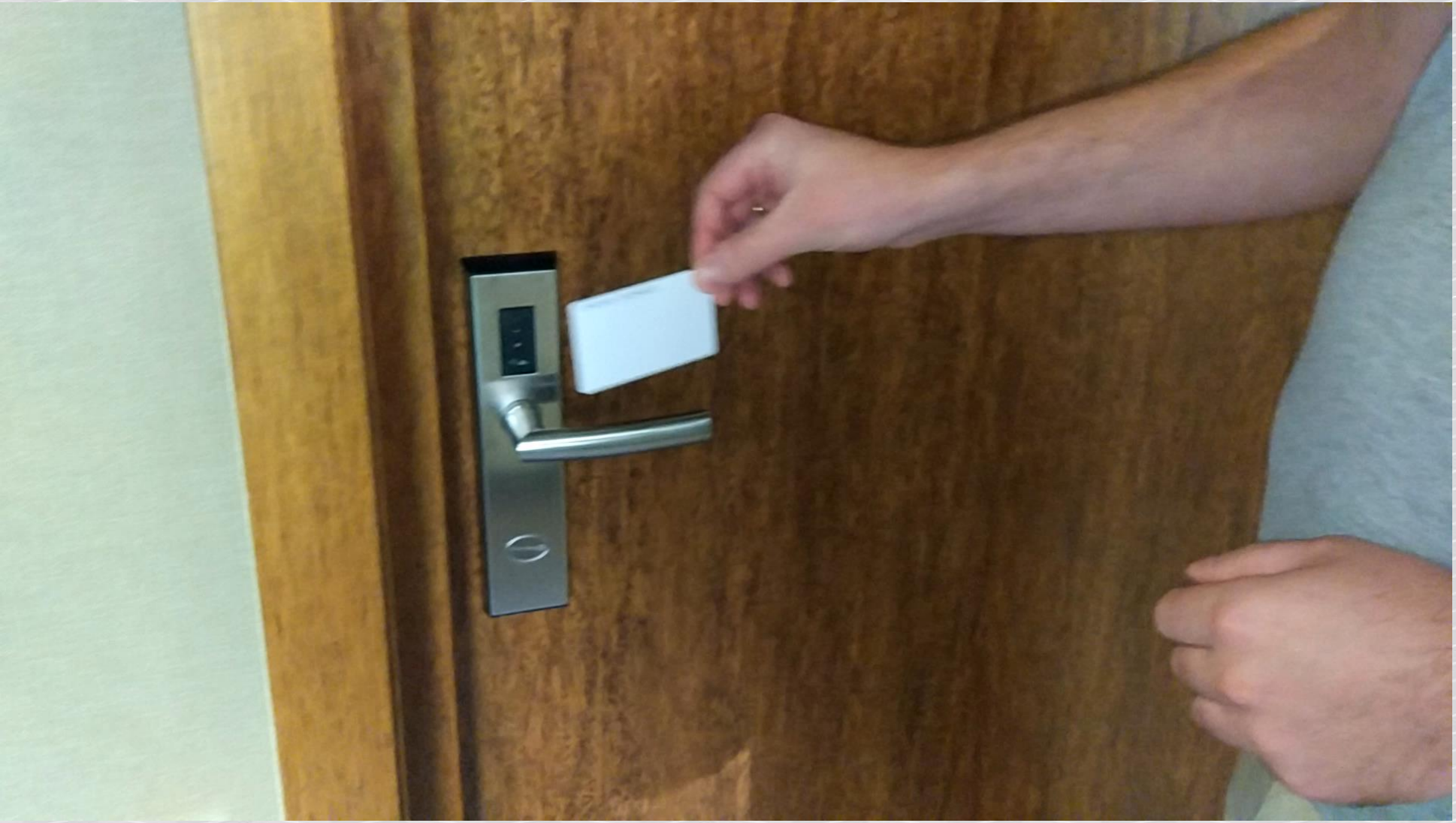
„Master" card?

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 ;)

https://giphy.com/gifs/the-lord-of-rings-lotr-fellowship-ring-JUPZtdfpu6srS

4-star hotel – unlock all the doors like a boss!



I'm really sorry but I could not resist...

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 ;)

https://giphy.com/gifs/embarrassed-facepalm-panda-14aUO0Mf7dWDXW

Crime scene card?

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

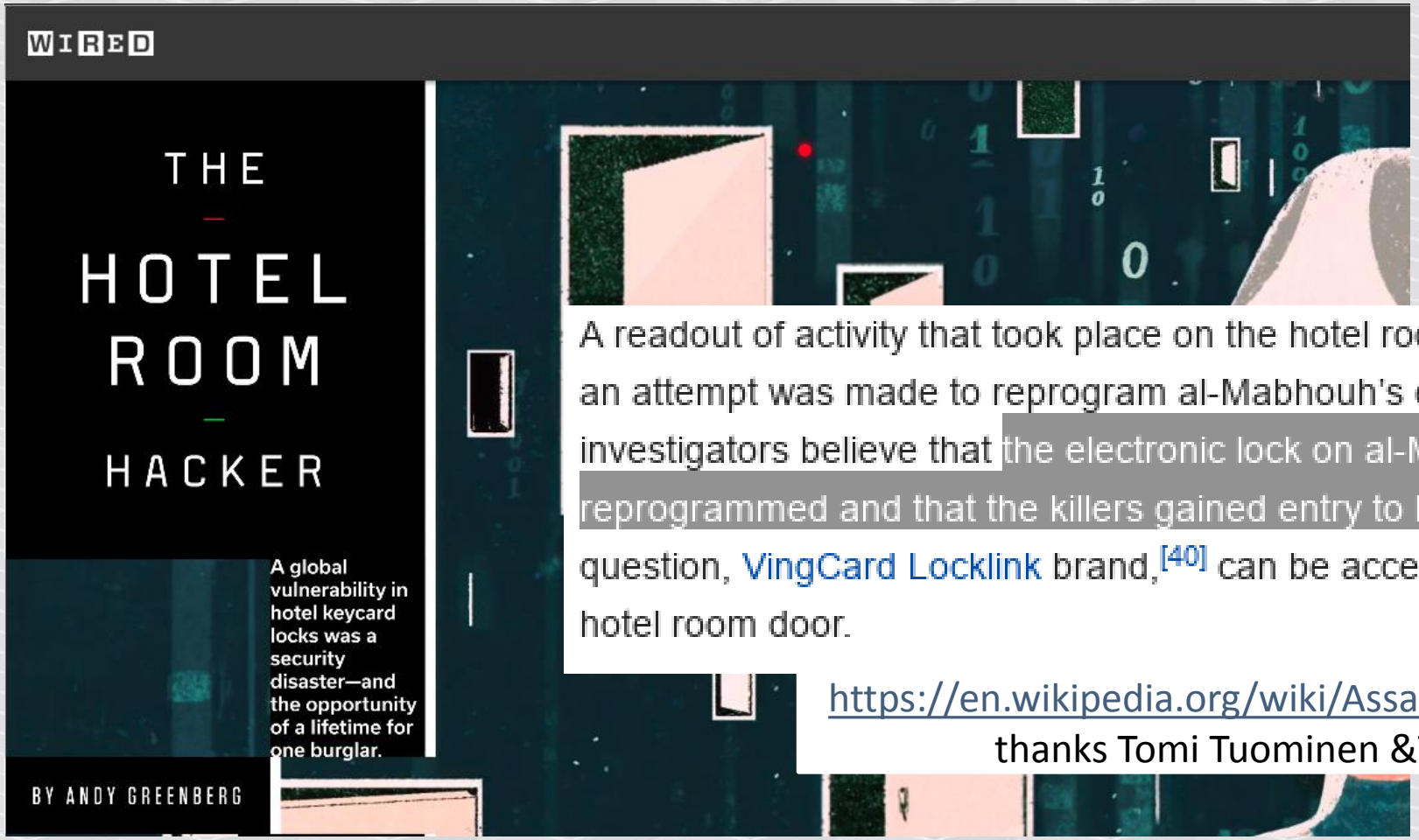
The police has to force the door open (break it).

Real risk?

Some hotels still use even more legacy systems.

Monitoring, guards, additional layers of security...

On the other hand...



Assassination of Mahmoud Al-Mabhouh

Location	Dubai, United Arab Emirates
Date	19 January 2010

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.[39] The locks in question, VingCard Locklink brand,[40] can be accessed and reprogrammed directly at the hotel room door.

https://en.wikipedia.org/wiki/Assassination_of_Mahmoud_Al-Mabhouh

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/

https://play.google.com/store/apps/details?id=au.id.micolous.farebot

Supported cards / agencies

Card / Agency	Location
Bilhete Único	São Paulo, Brazil
Clipper	San Francisco, CA, USA
Cubic Nextfare	*many locations*
Edy	Japan
ERG	*many locations*
EZ-Link	Singapore
Go card	Brisbane and South East Queensland, Australia
Manly Fast Ferry	Sydney, NSW, Australia
Matkakortti, HSL	Finland
Metrocard	Christchurch, New Zealand
Myki	Melbourne (and surrounds), VIC, Australia
MyWay	Australian Capital Territory, Australia
NETS FlashPay	Singapore
Octopus	Hong Kong
Opal	Sydney (and surrounds), NSW, Australia
ORCA	Seattle, WA, USA
OV-chipkaart	Netherlands
Shenzhen Tong	Shenzhen, Guangdong Province, China
SmartRider	Western Australia, Australia
Suica, ICOCA, PASMO	Japan
Transit Access Pass	Los Angeles, CA, USA

Metrodroid – reversing process

Finding the balance

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

gocard-2015xxxx_yyyy.mfc

0000 0040: 01 31 74 02  $6.28  4 00  00 00 00 00 00 34 01 50  .!..t.4. .....4.P
0000 0050: 01 31 3A 01  $3.14  4 00  00 00 00 00 00 3A 48 CF  .!:....t. .....:..

gocard-2015xxxx_yyyy.mfc

0000 0040: 01 31 0A 09  $23.14 8 00  00 00 00 00 00 42 2F 1D  .!..Vx.. .....B/.
0000 0050: 01 31 3A 01  $3.14  4 00  00 00 00 00 00 3A 48 CF  .!:..... .....:..
```

Balance (cents)

Priority

Checksum

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

City cards fraud?

Aplikacja do nielegalnego ładowania Warszawskiej Karty Miejskiej za BTC

Adam Haertle dodał 31 marca 2013 o 17:10 w kategorii Krypto, Mobilne, Prawo z tagami: Mifare • NFC • Warszawa • ZTM

Słabość zabezpieczeń kart Mifare Classic, z którym korzysta między innymi warszawski ZTM, jest znana od wielu lat. Kwestią czasu było pojawienie się na rynku powszechnie dostępnej alternatywnej usługi ładowania kart miejskich. Ta chwila właśnie nadeszła.

Do tej pory Warszawskie Karty Miejskie ładowane były przez domorosłych elektroników na zasadzie przysługi znajomi-znajomym. Choć jak do tej pory w sieci nie pojawiła się dokładna instrukcja jak krok po kroku przeprowadzić cały proces, to ilość dostępnych materiałów jest w zupełności wystarczająca, by średnio uzdolniony informatyk opanował ładowanie kart ZTM w ciągu kilku godzin.

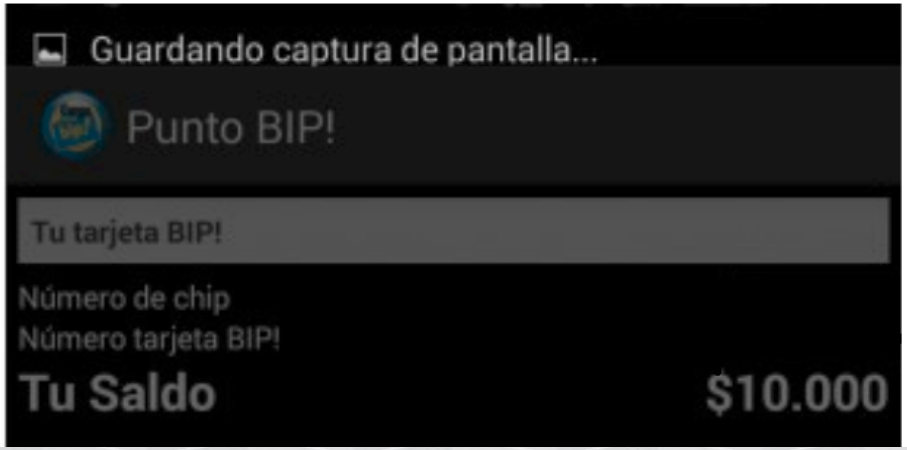
https://zaufanatrzeciastrona.pl/post/aplikacja-do-nielegalnego-ladowania-warszawskiej-karty-miejskiej-za-btc/

Android NFC hack allow users to have free rides in public transportation

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. 16 the very first widely-available app for Android appeared, allowing users to load these transportation cards with 10k Chilean pesos, a sum equal to approximately $17 USD.



https://securelist.com/android-nfc-hack-allow-users-to-have-free-rides-in-public-transportation/67283/

‘Sophisticated’ £370,000 Oyster card fraud sees Seven Kings man jailed for six years and nine months

PUBLISHED: 08:21 24 October 2017 | **UPDATED:** 08:21 24 October 2017

Matthew Clemenson

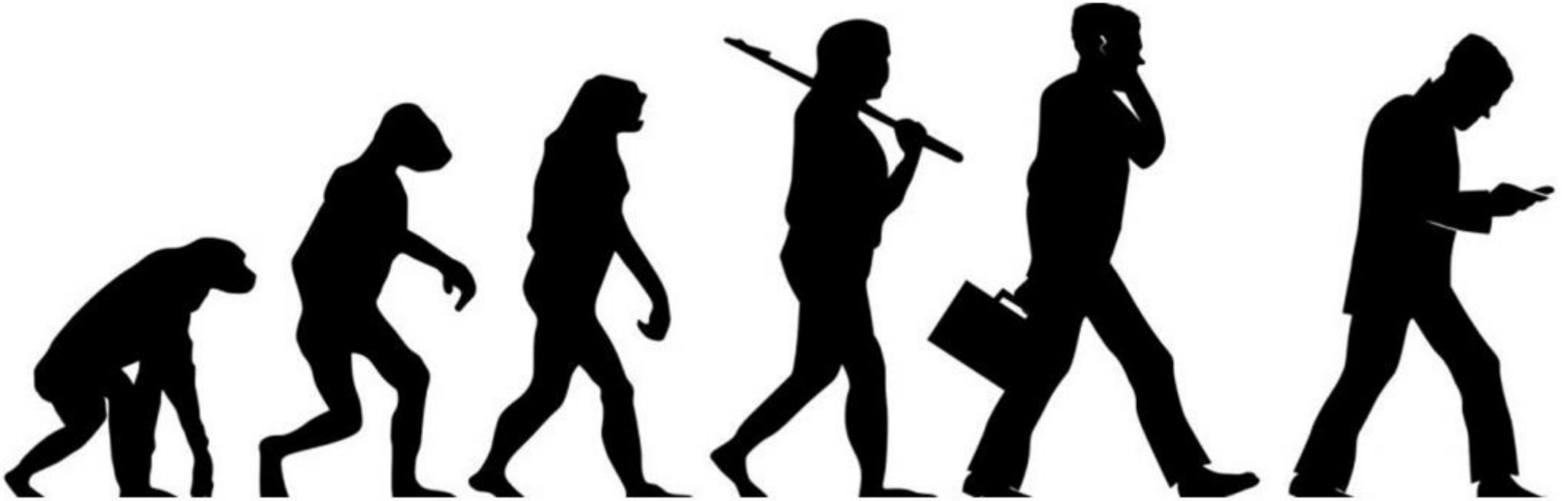
Nathan Jeffrey-Payne, 28, of Nutfield Gardens, Seven Kings, was part of a six-strong gang of sophisticated criminals who found a way to clone older Oyster cards and trick ticket machines into thinking there was still money on them.

These fraudulent first generation Oysters were then used at multiple ticket machines across London to obtain thousands of pounds in false refunds.

http://www.ilfordrecorder.co.uk/news/crime-court/sophisticated-370-000-oyster-card-fraud-sees-seven-kings-man-jailed-for-six-years-and-nine-months-1-5249071

MOBILE ACCESS

Evolution goes mobile

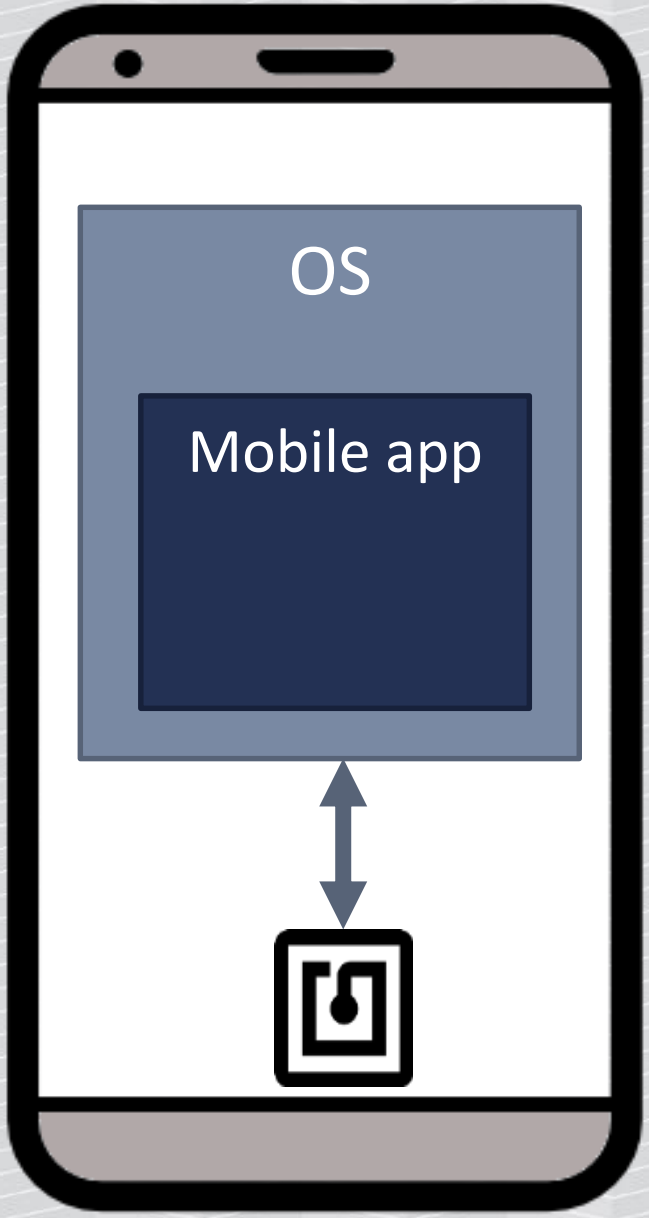


Host Card Emulation

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).



iOS?

EXCLUSIVE CYBERSECURITY APPLE

Apple to Expand Secure Wireless Chip Beyond Payments

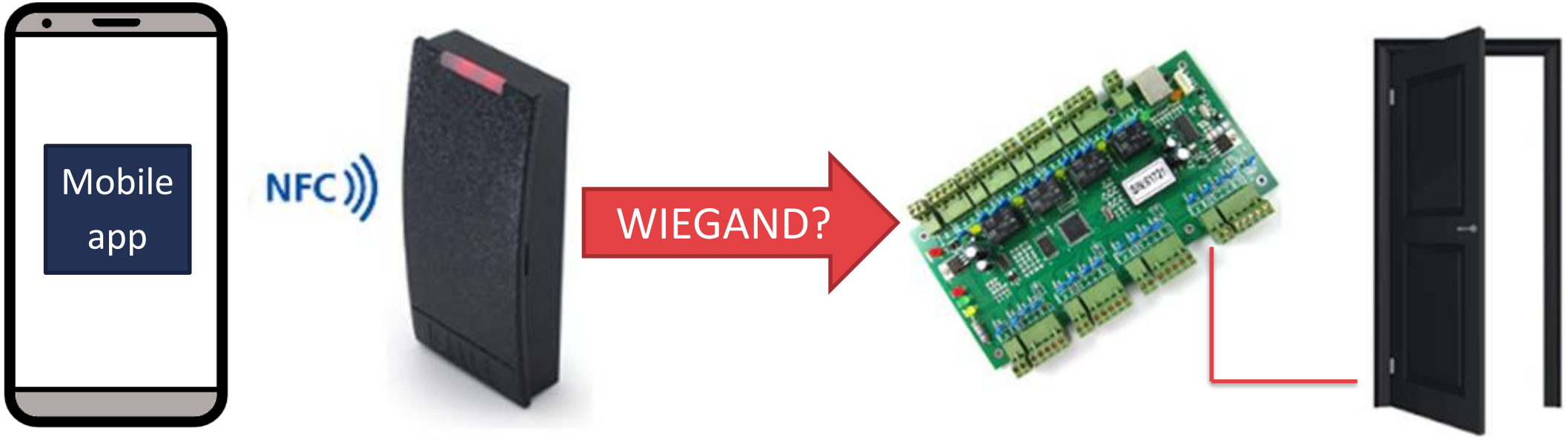
By Aaron Tilley and Amir Efrati May 25, 2018 4:32 PM PDT · Comments by Joshua Bernstein and Benedikt Roßgardt

Subscribe now

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.

https://www.theinformation.com/articles/apple-to-expand-secure-wireless-chip-beyond-payments

How does it work? (most cases)



How does it work? (most cases)

Mobile app stores:

- Key to the reader (usually per-installatio
- Individual user ID

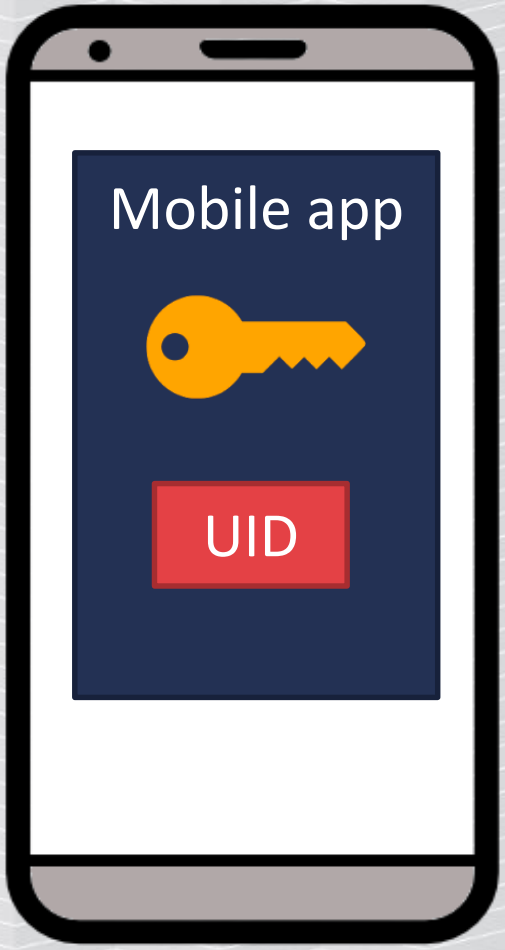
What could possibly go wrong?

Mobile malware – steals the access data.

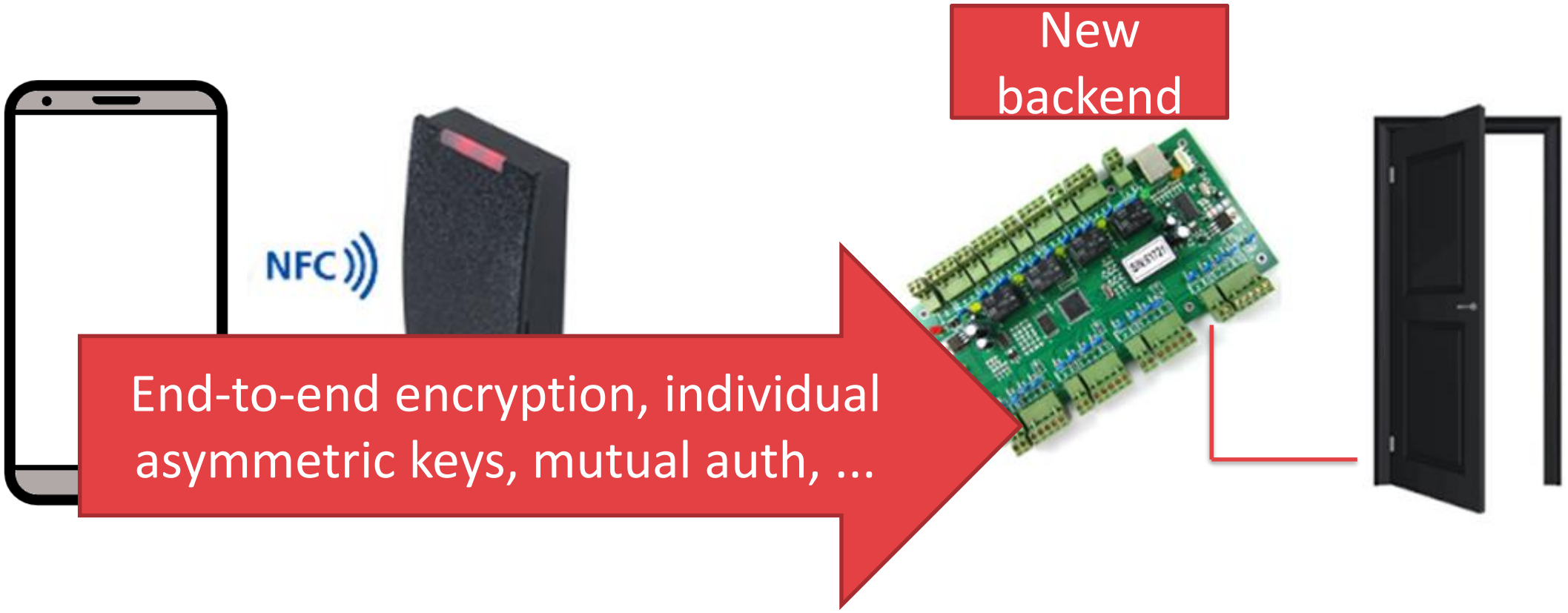
Malicious user – tampers his own ID and gets access to restricted areas.

Administrative access – reader reconfiguration.

More info soon…



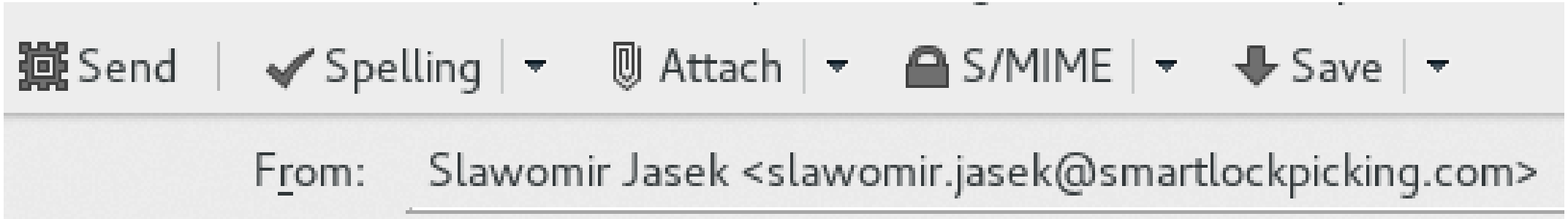
New possibility to make it right?



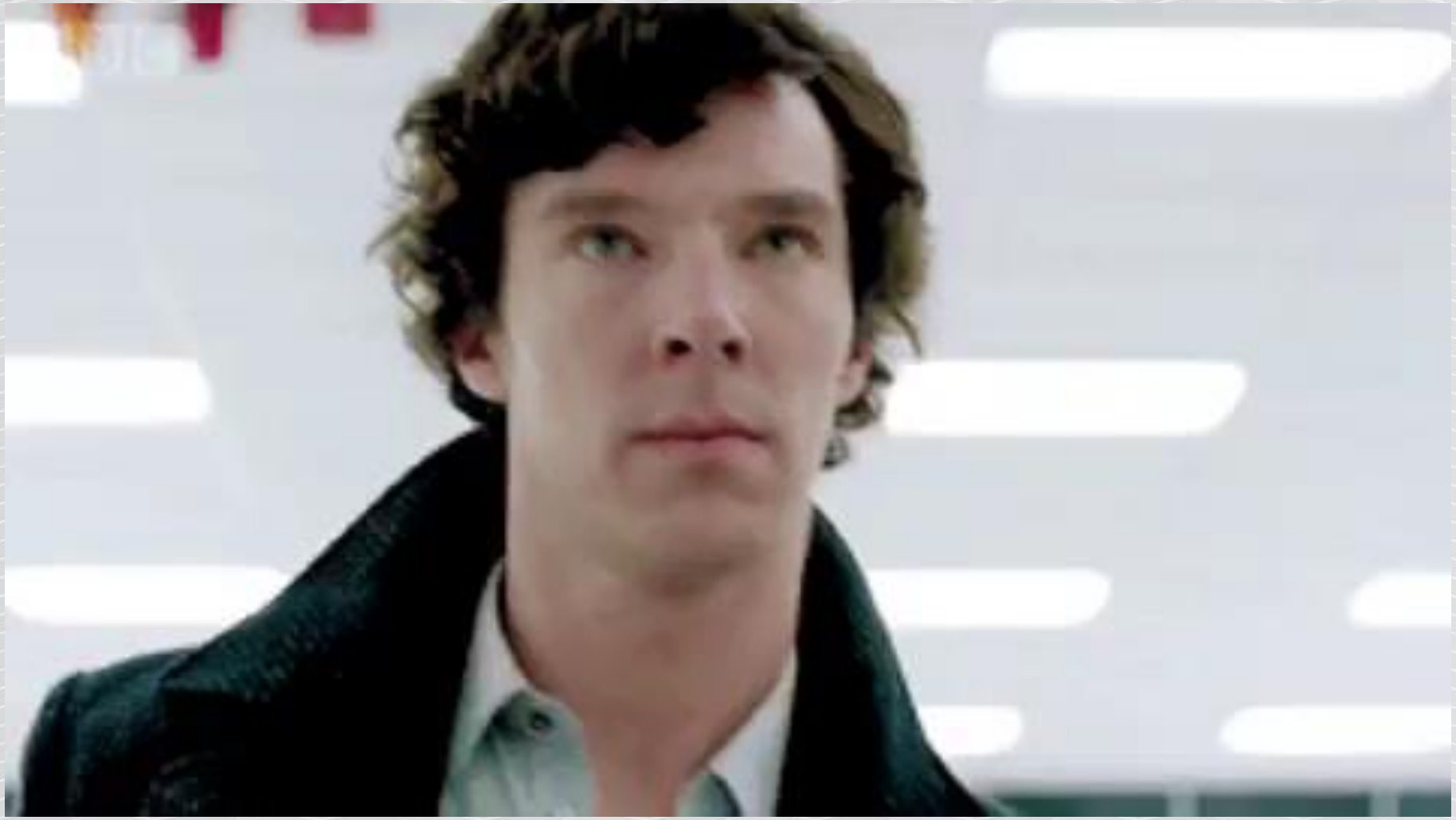
Not easy to get such system...

Hello Slawomir,

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

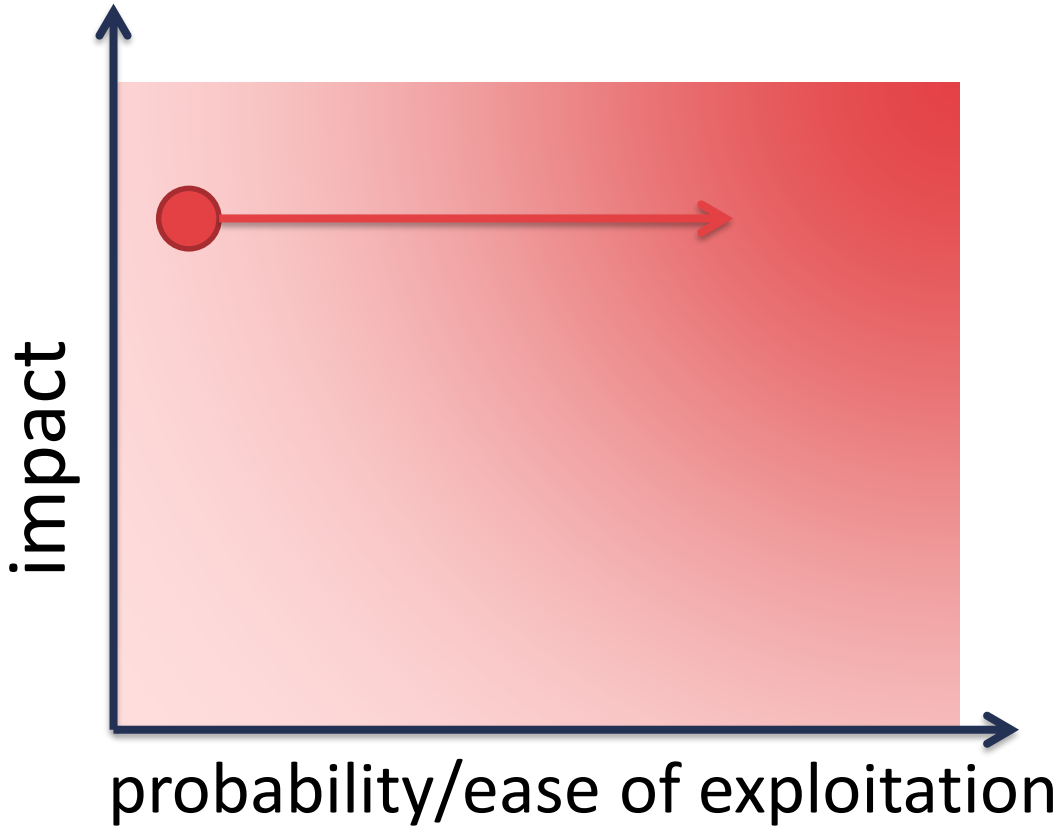


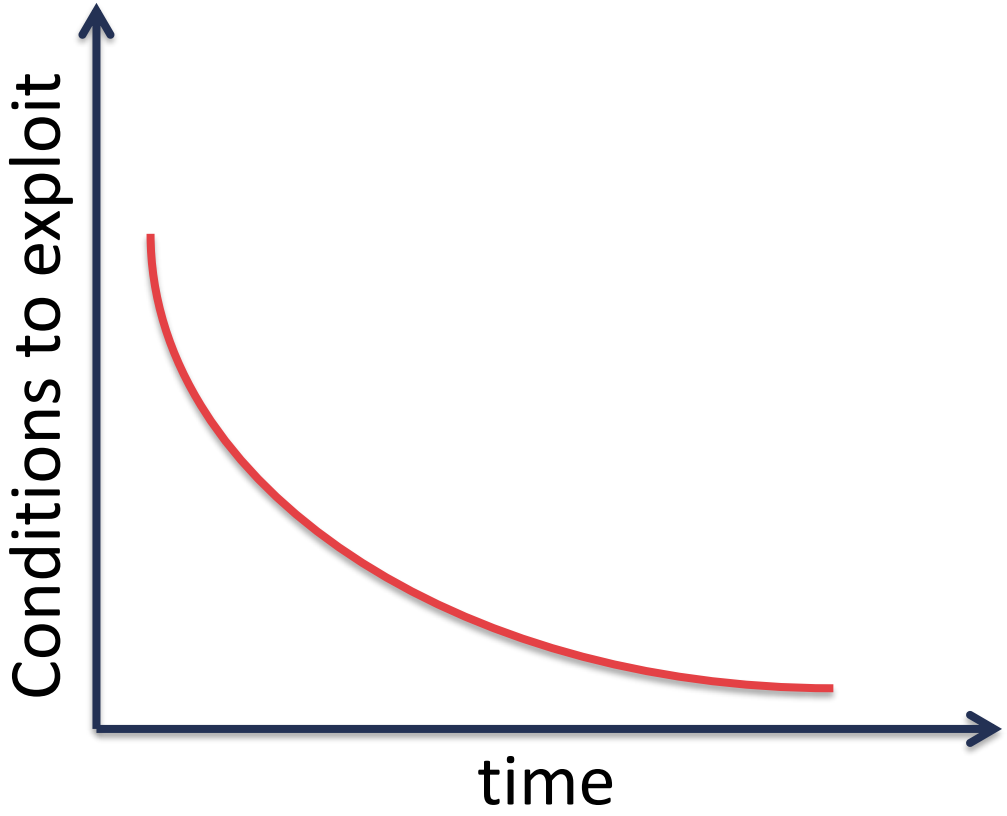
Time…



https://giphy.com/gifs/sherlock-bbc-one-l0MYGtCMbPTYWOzaU

Risk?


impact
probability/ease of exploitation

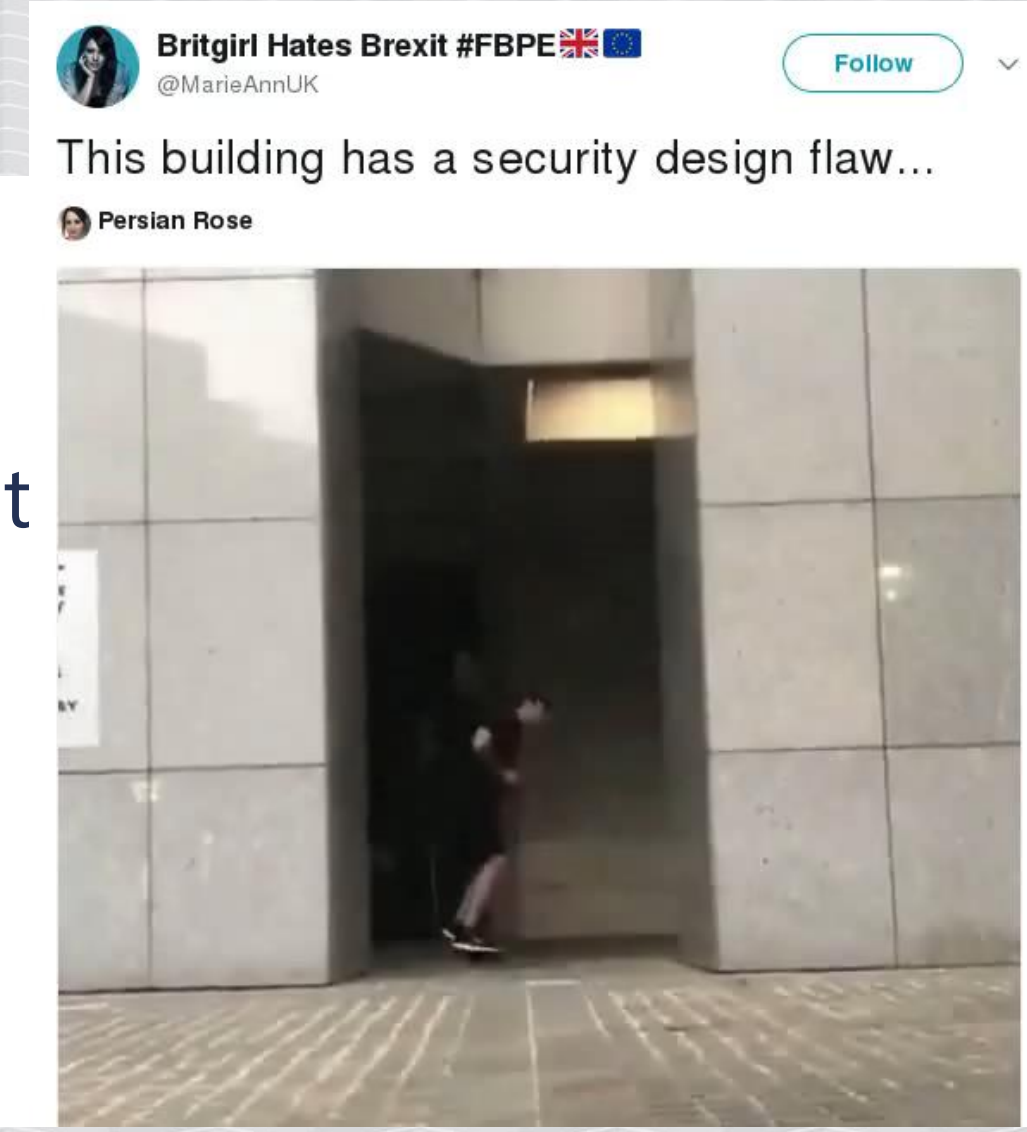

Conditions to exploit
time

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.



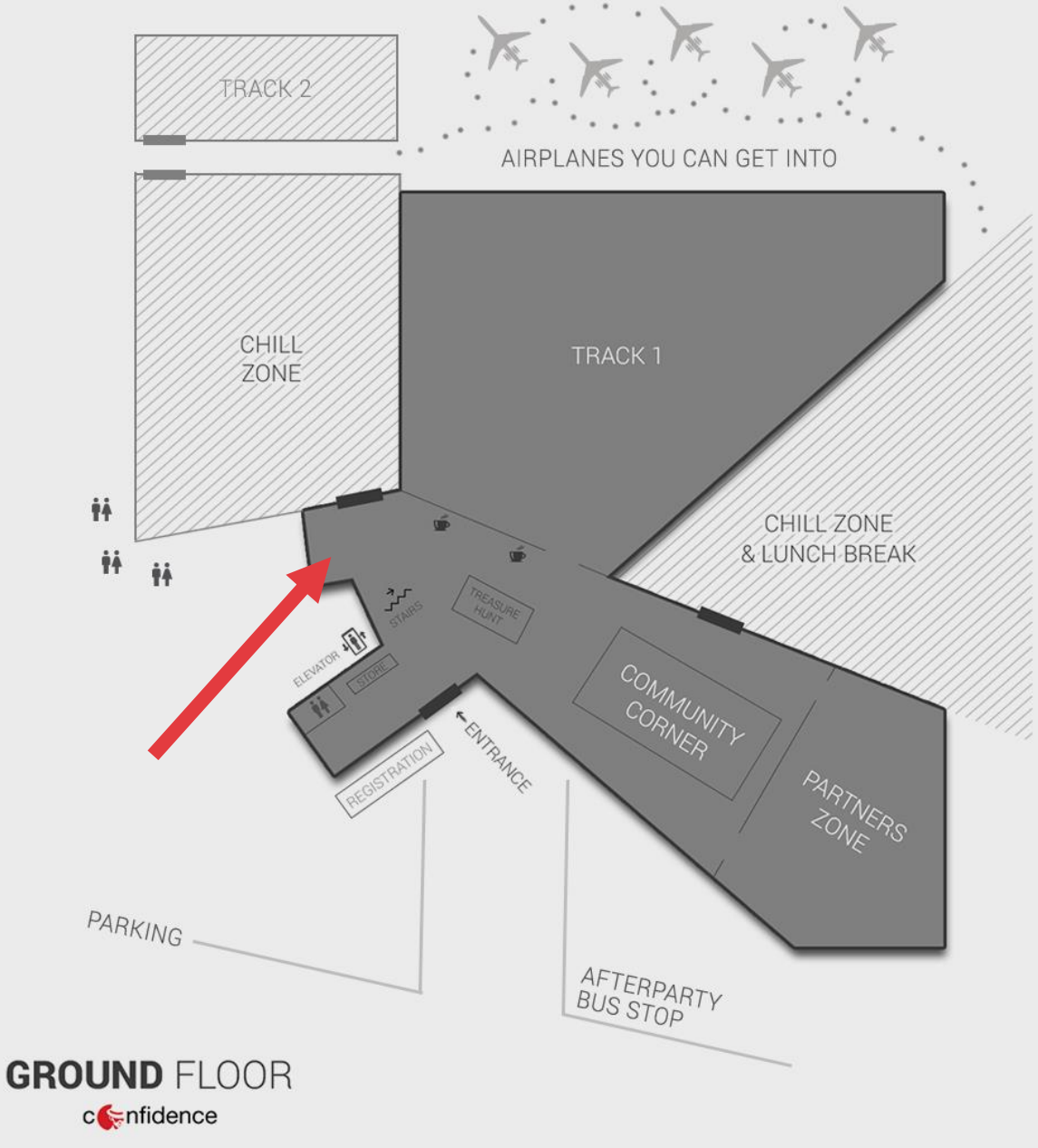
https://twitter.com/MarieAnnUK/status/924671277507469313

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

securing

<15 yrs>

MORE THAN SECURITY TESTING

Thank you! Questions?

Slawomir.Jasek@securing.pl slawekja