ROSEN Digital Business Solutions

Front door nightmares

-when smart is not secure

ROSEN-DBS.COM
From Data to Information to Decisions

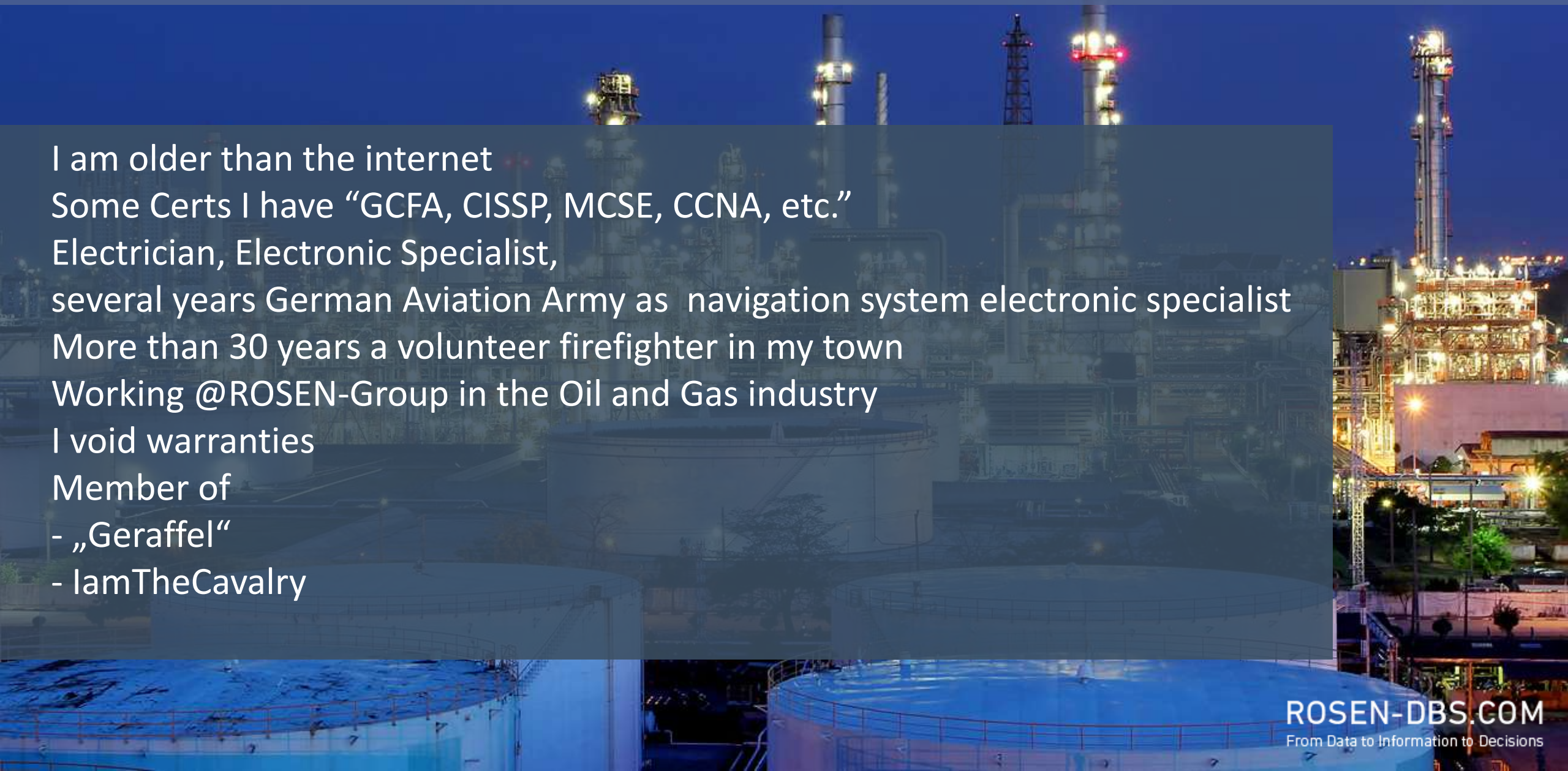
disclaimer

- This content is not for burglars
- Research only my own locks
- I had only one sample of each of the locks

Agenda

- Who am I
- Why Electronical Door Locks
- How they work
- Attack Vectors
- 5 scenarios
- What can we do
- fails

who am I

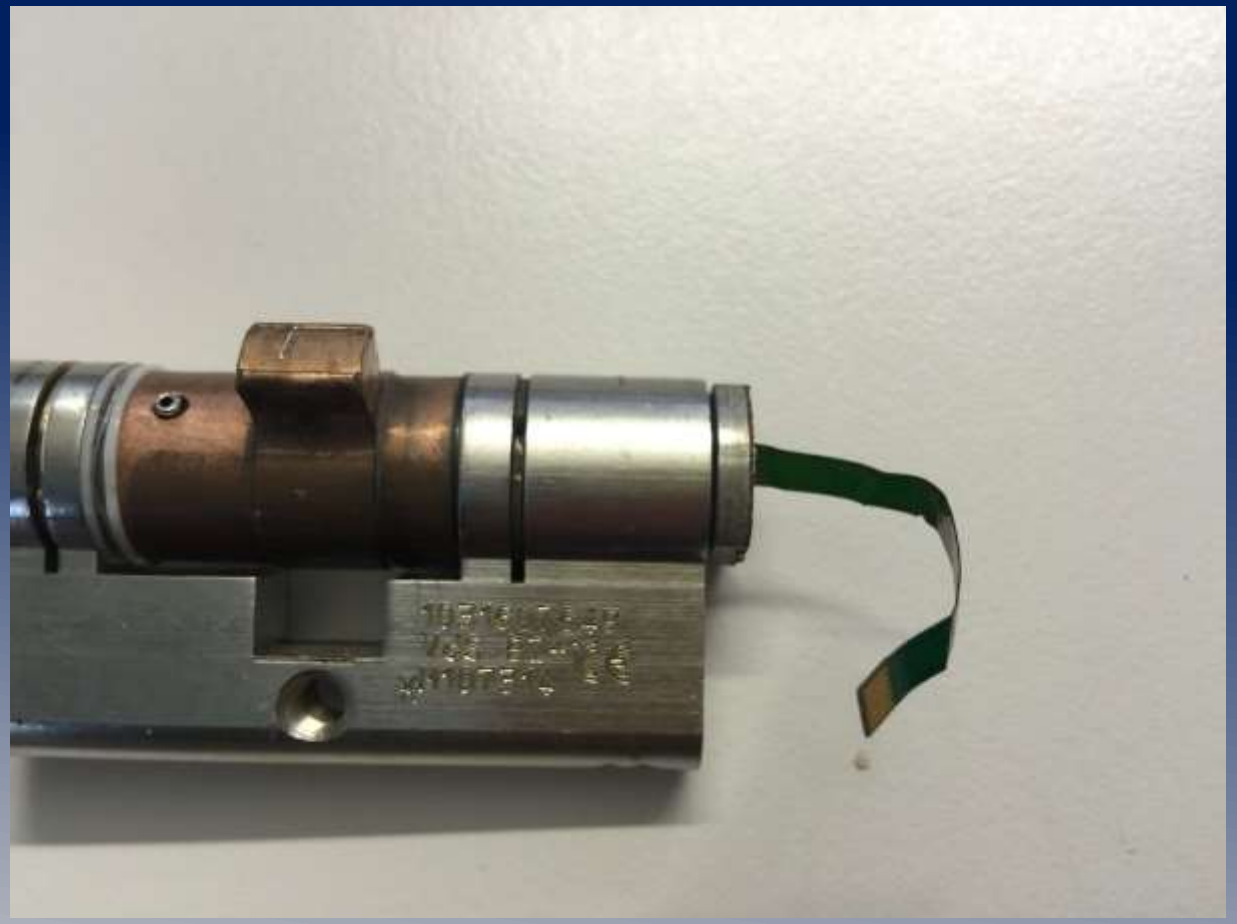


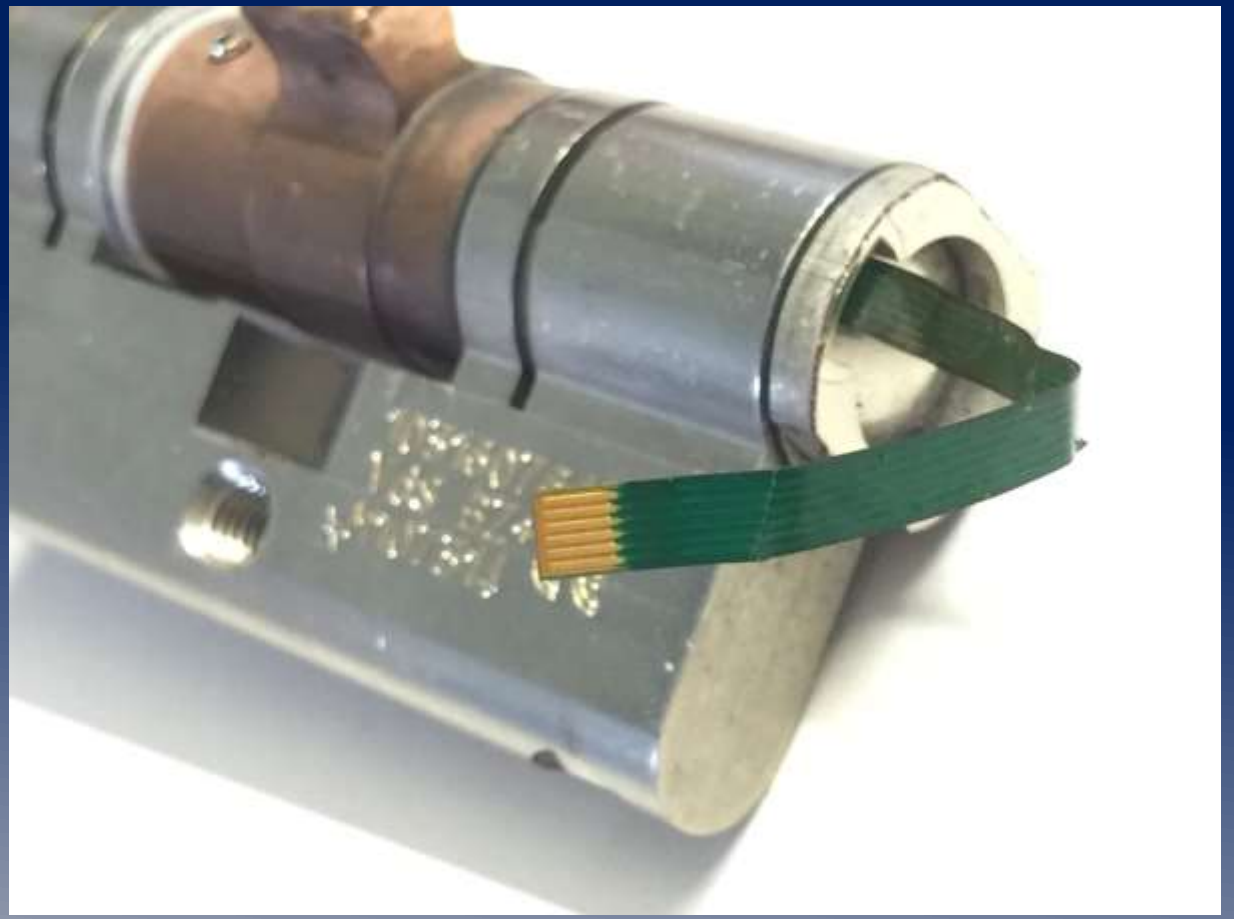
I am older than the internet
Some Certs I have “GCFA, CISSP, MCSE, CCNA, etc.”
Electrician, Electronic Specialist,
several years German Aviation Army as navigation system electronic specialist
More than 30 years a volunteer firefighter in my town
Working @ROSEN-Group in the Oil and Gas industry
I void warranties
Member of
- „Geraffel“
- IamTheCavalry

Business segments of ROSEN

- Through our business activities, we help customers to avoid leaks and spills by inspecting facilities, pipelines and tanks
- We have inspected billions of square meters of Oil- and Gas-Pipelines with ultrasound, eddy current, magnetic flux leakage, optical and acoustic technologies, worldwide.
- We focused on safety and security of humans and environment
- ROSEN not only serves the oil and gas industry but also aerospace, marine, transportation and security

Why this topic?
A broken lock caught my attention





Why electronic door locks

Why electronic (smart) locks ?

Idea behind it is to make key management easy

- Loosing a key now ≠ replacing whole lock
- Just delete the allowed transponder and add a new one
- Time restrictions possible
- Easy to implement and replace classic locks
- Classical locks extended or combined with RFID, NFC or WiFi

Transponder Available from LF Em4x02 cards over Hitags-s to HF Mifare EV1/2

Focusing onto this type smart Door locks

Basic principle

something you have

- RFID Transponder is the key

Something you are

- Fingerprint or other biometrics

something you know

- Pin Pad

2FA possible, Transponder and a PIN Pad or other combinations

Lock electronic compares what you have or know with stored allowed ID’s

If ID is allowed – door will open , after couple of seconds, door is locked again

General design

outside = electronics & RFID reader on “unsafe” outside
inside = electronics & RFID reader on the “safe inner side”
Mixed configuration

Locking and unlocking mostly done by magnetic fields.

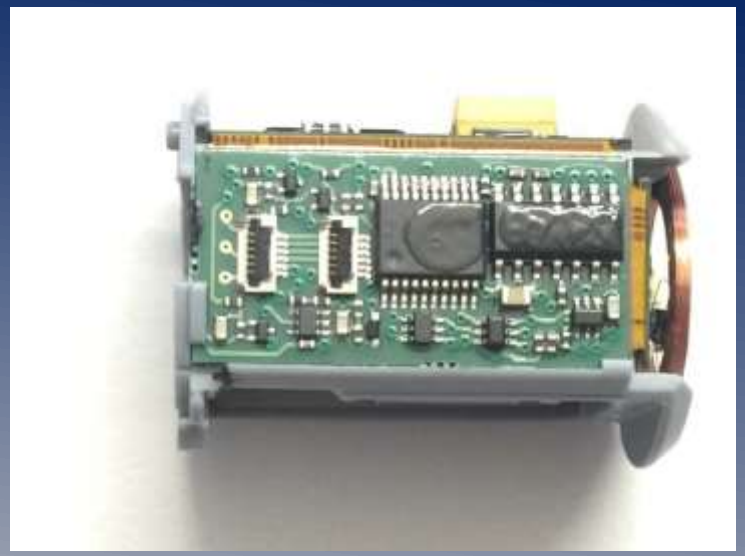
- Magnets (positioned by a motor in a defined position)
- Electromagnet coil (moving a bolt)

Some using a motor to move mechanic parts

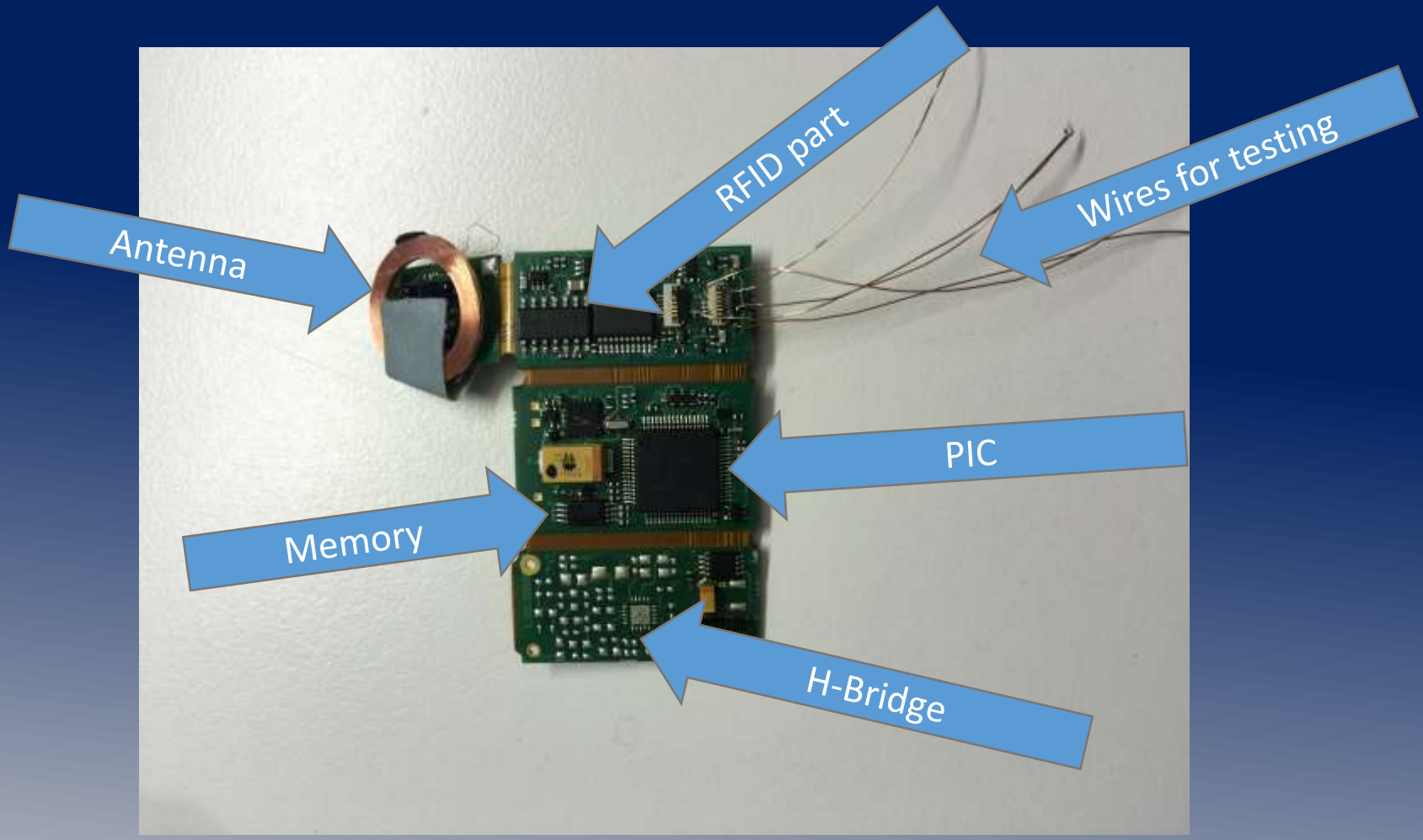
How they work

The electronic Parts

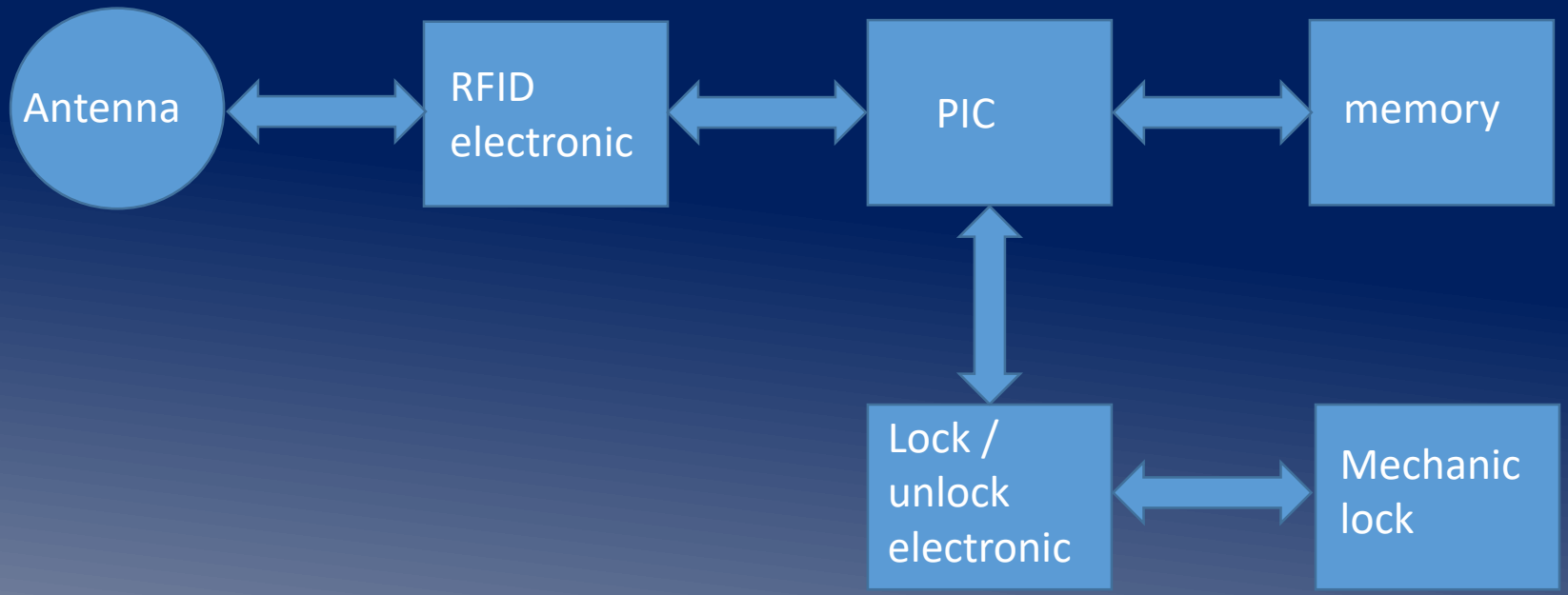
“intelligence” or „Brain“ of the lock



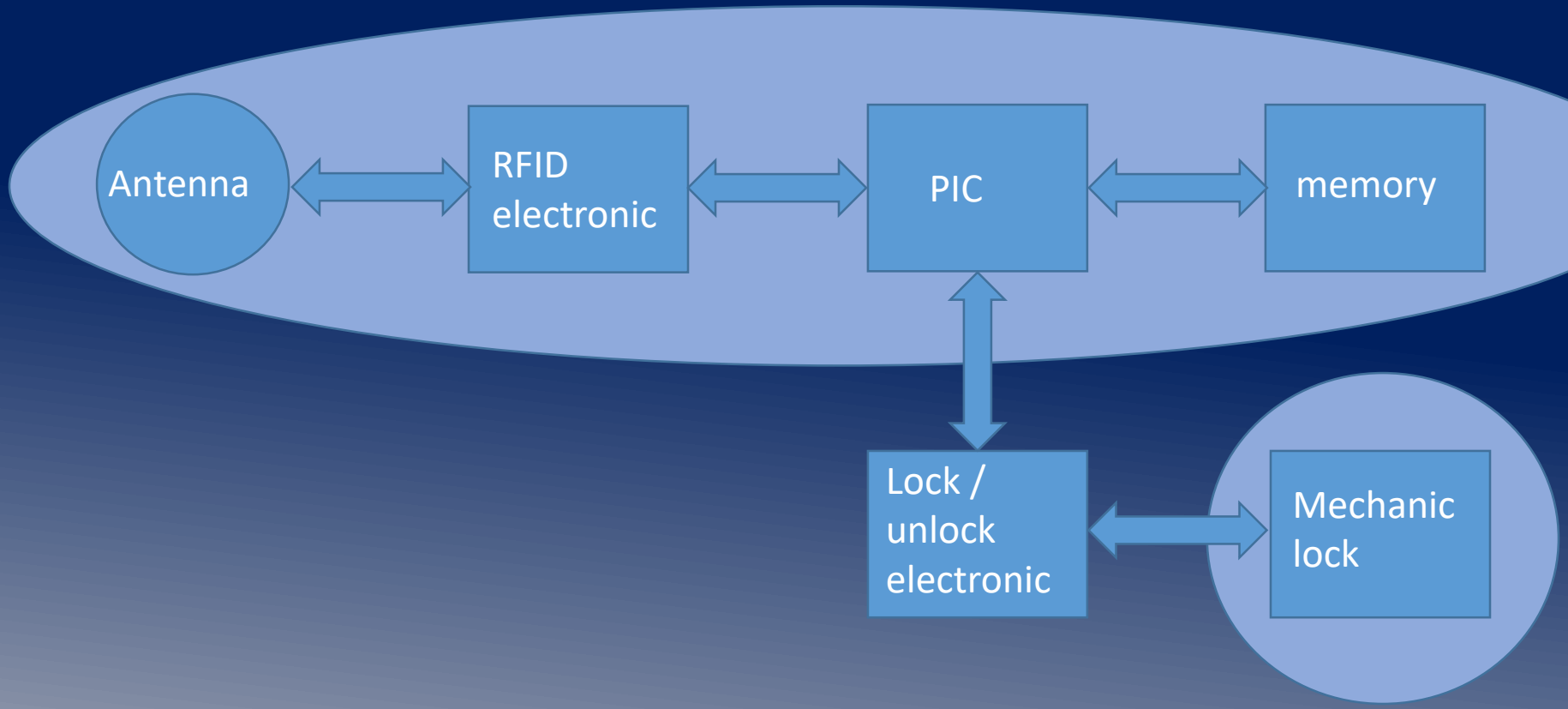
Main parts of the electronic



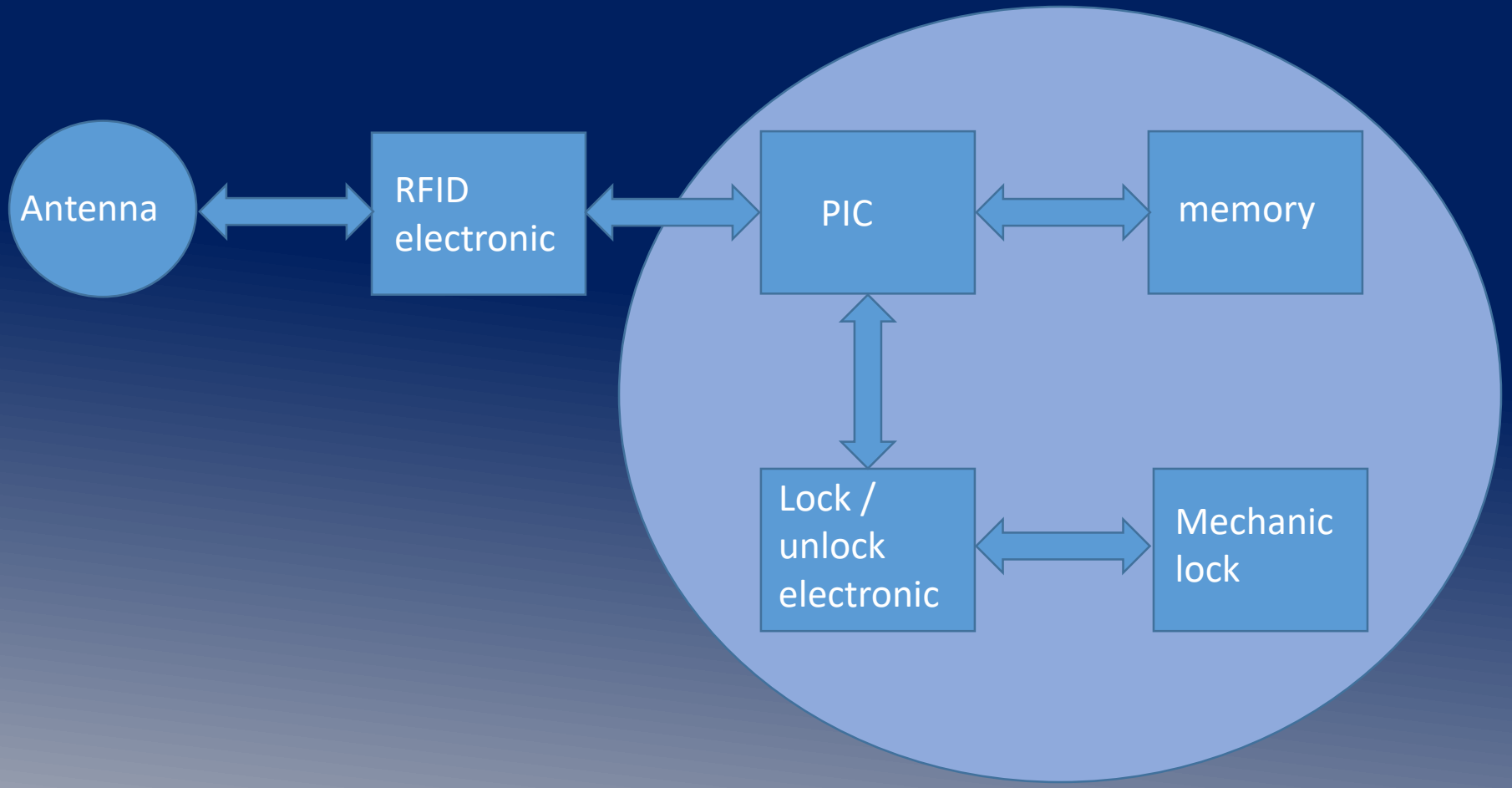
Block Diagram



Known attack vectors



My research focus

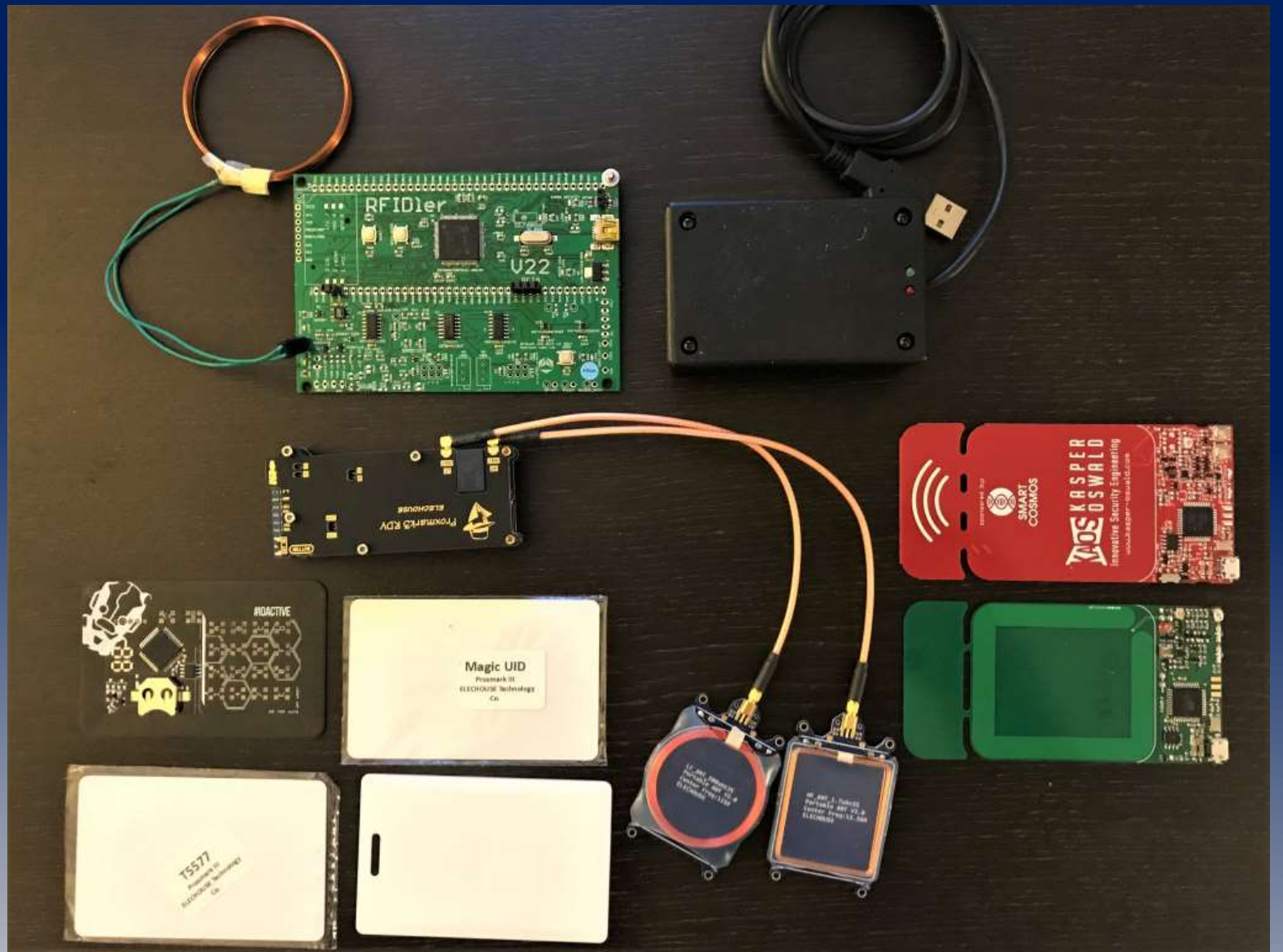


RFID Part

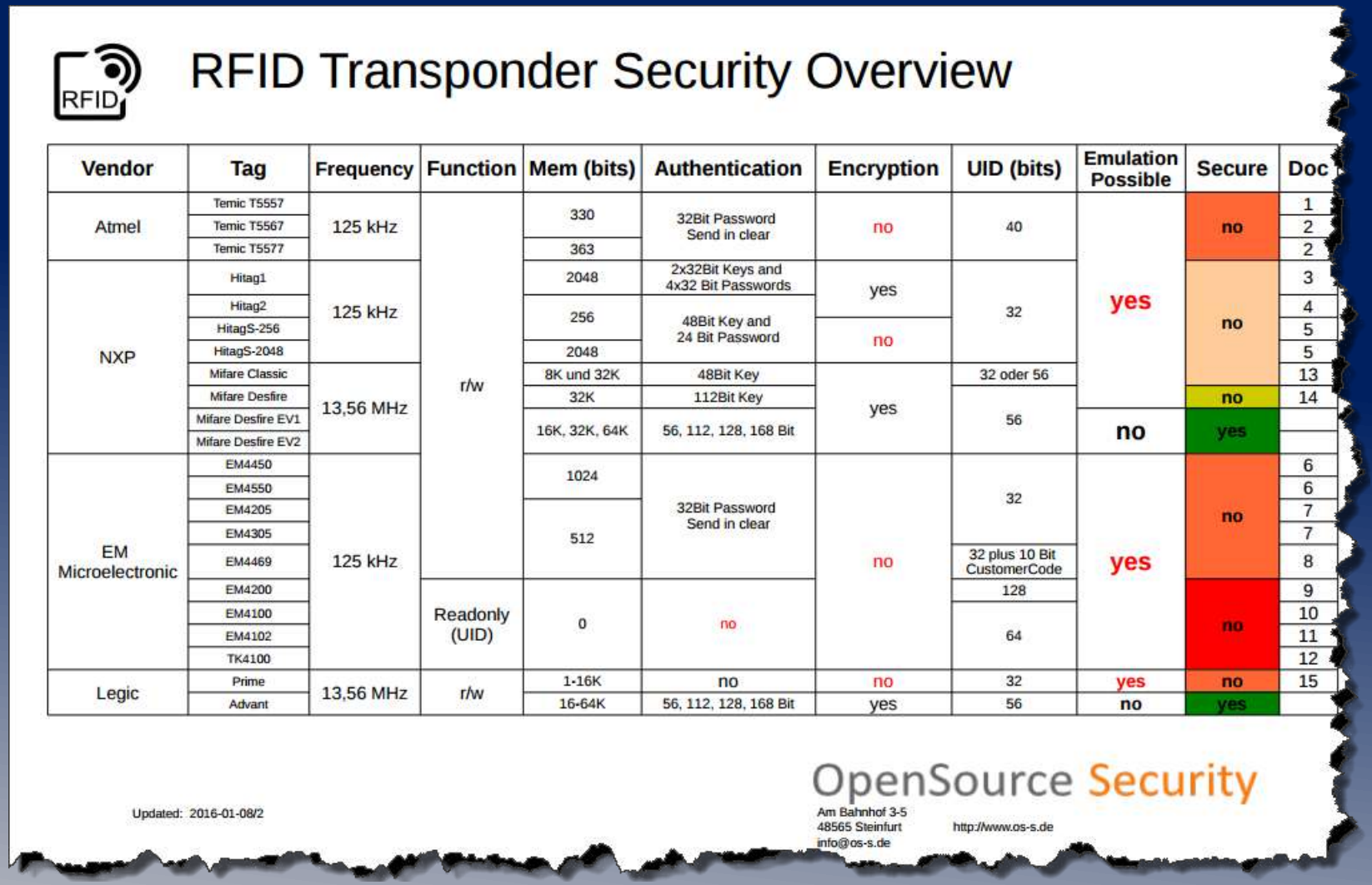
Tools for RFID based attacks

125 kHz Low frequency
- RFIDler
- LAHF
- Proxmark III
- Em410x emulator

13.56 MHz High frequency
- LAHF
- Proxmark III
- Chameleonmini



RFID Transponder Security overview



RFID Transponder Security Overview

Vendor	Tag	Frequency	Function	Mem (bits)	Authentication	Encryption	UID (bits)	Emulation Possible	Secure	Doc
Atmel	Temic T5557	125 kHz	r/w	330	32Bit Password Send in clear	no	40	yes	no	1
	Temic T5567									2
	Temic T5577			363						2
NXP	Hitag1	125 kHz		2048	2x32Bit Keys and 4x32 Bit Passwords	yes	32		no	3
	Hitag2			256	48Bit Key and 24 Bit Password					4
	HitagS-256					no				5
	HitagS-2048			2048						5
	Mifare Classic	13,56 MHz		8K und 32K	48Bit Key	yes	32 oder 56			13
	Mifare Desfire			32K	112Bit Key		56		no	14
	Mifare Desfire EV1			16K, 32K, 64K	56, 112, 128, 168 Bit			no	yes	
	Mifare Desfire EV2									
EM Microelectronic	EM4450	125 kHz		1024	32Bit Password Send in clear	no	32	yes	no	6
	EM4550									6
	EM4205			512						7
	EM4305									7
	EM4469						32 plus 10 Bit CustomerCode			8
	EM4200		Readonly (UID)	0	no		128		no	9
	EM4100						64			10
	EM4102									11
	TK4100									12
Legic	Prime	13,56 MHz	r/w	1-16K	no	no	32	yes	no	15
	Advant			16-64K	56, 112, 128, 168 Bit	yes	56	no	yes	

Updated: 2016-01-08/2

OpenSource Security

Am Bahnhof 3-5
48565 Steinfurt
info@os-s.de

http://www.os-s.de

https://os-s.net/transponder-overview.pdf

Secure transponder (so far)

- most Transponder Types are “broken”
- “so far ” only 2 left

Legic Advance

Mifare Desfire EV1/2

Both are HF Transponder with NFC Frequency 13.56 MHz

Only a nice sample?

Software Bug in crypto of the active Transponder

a sample:

- active Transponder with 128 AES encryption
- faulty implementation of the RND
- RNG used 40 bit of the 128 Bit AES Masterkey and sends to the key
- PoC sends 5 requests and had the complete masterkey to make his own ones
- Vendor patched with a firmware update

Digging deeper into the locks

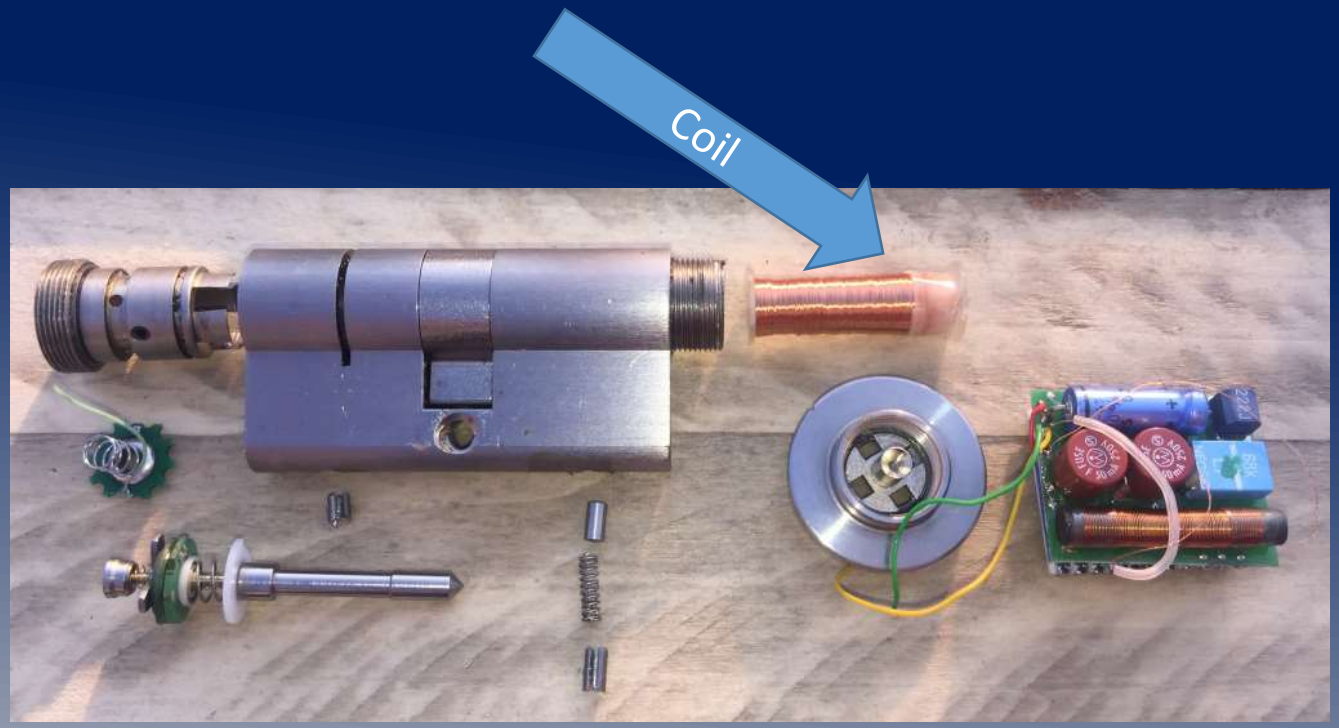
Electromechanical functioning

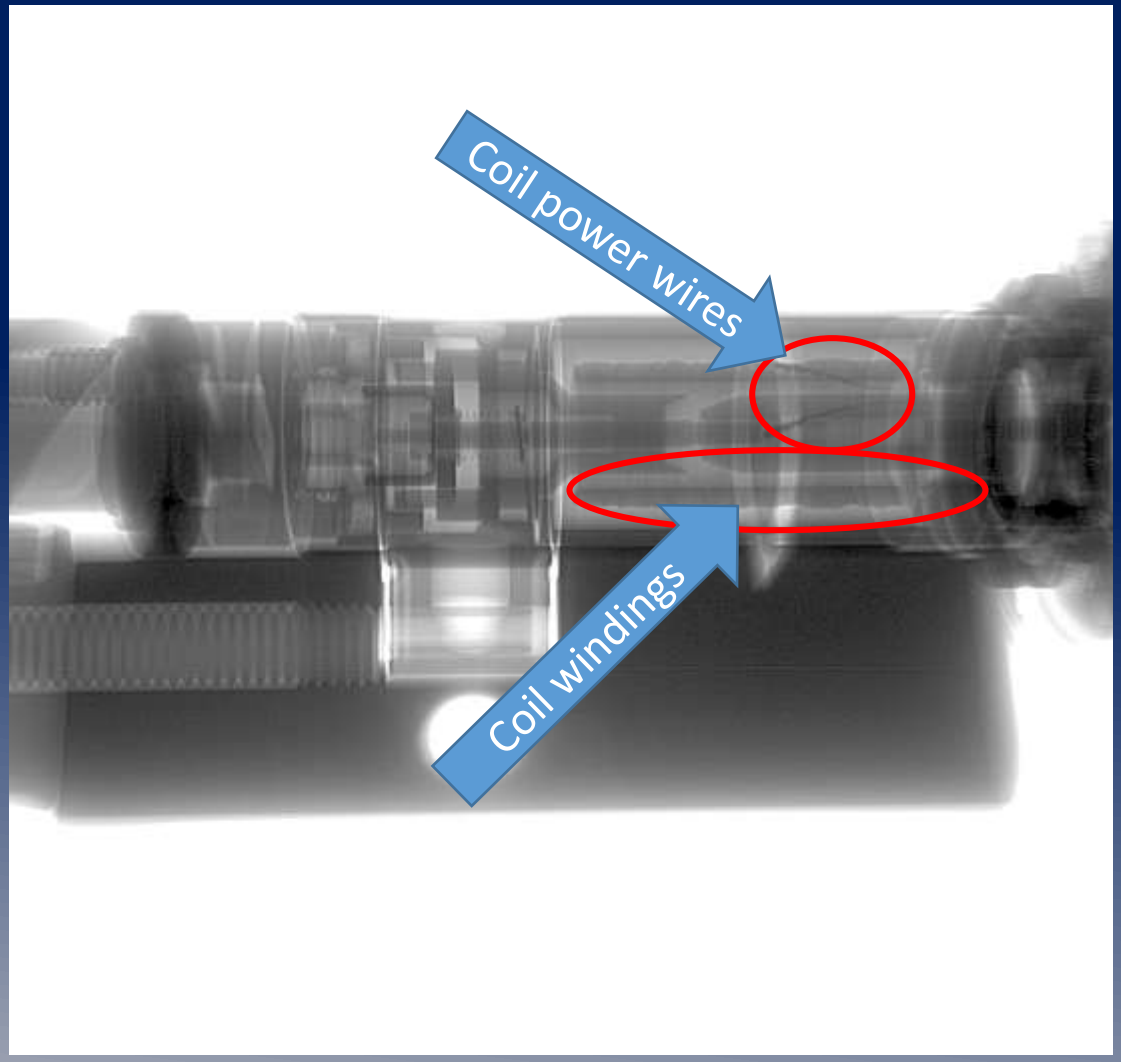
Unlocking mechanism

I currently only know 4 different types

- Magnets, positioned by a electro motor
- Electro motor that mechanically locks
- Magnetic field, created by a coil
- some locks have a bypass or emergency key!

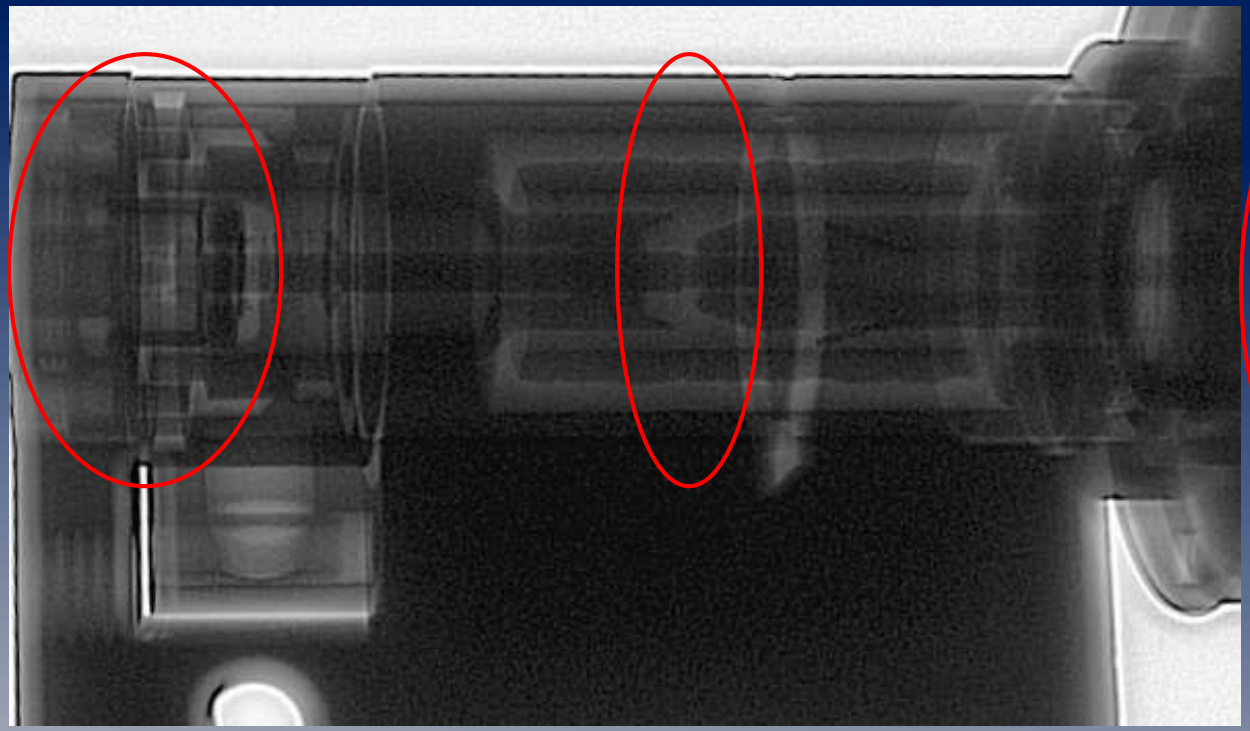
X-Ray makes things easy



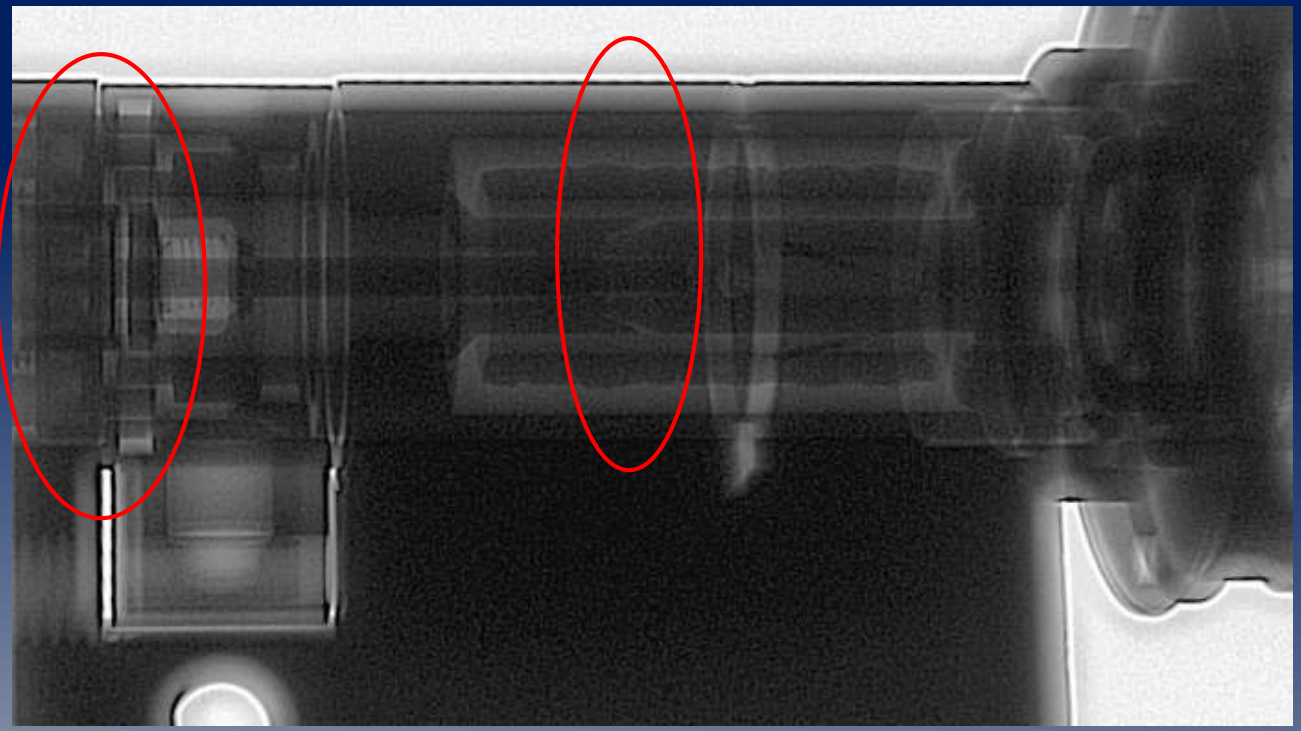


Unlocking with Electromagnetic field

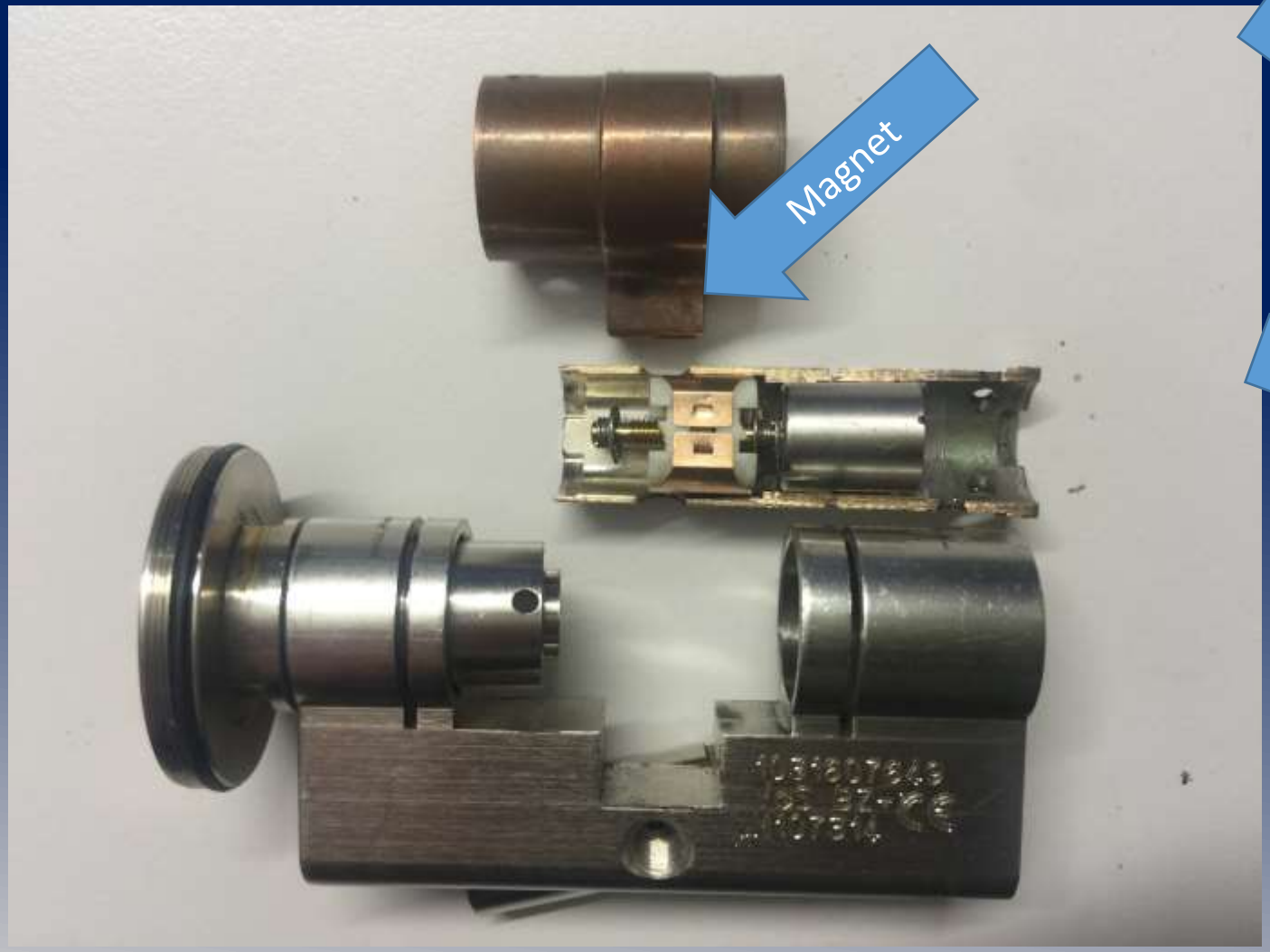
locked



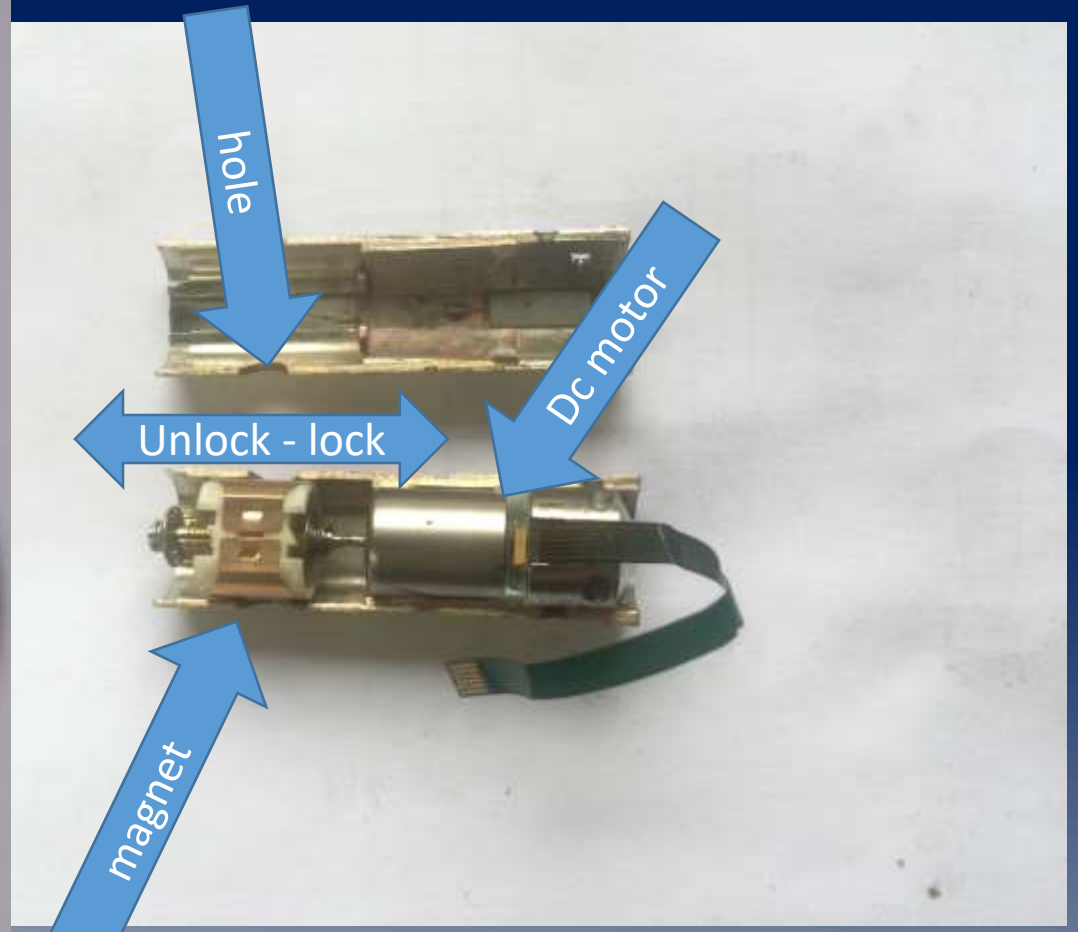
open



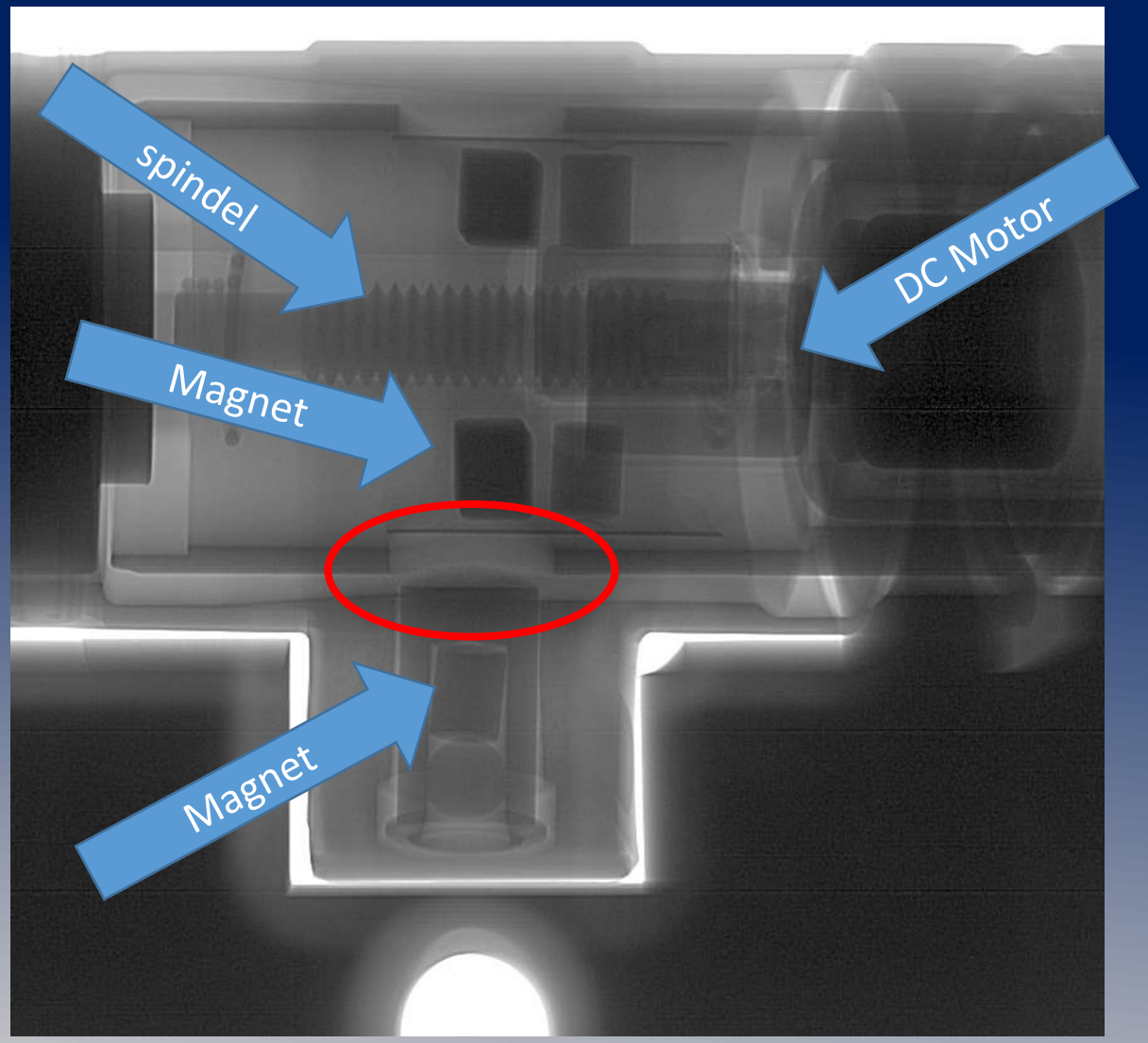
magnets and dc motor

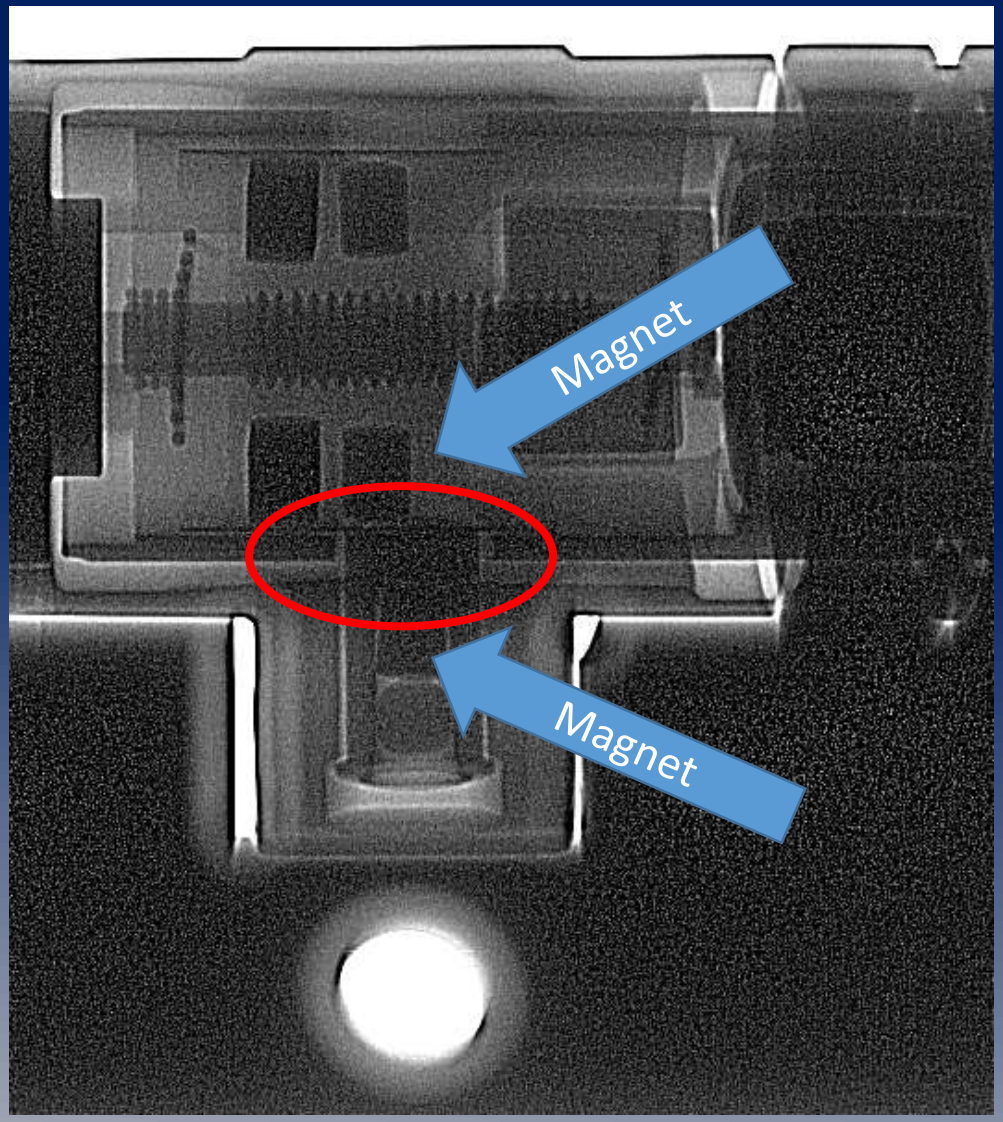


magnets

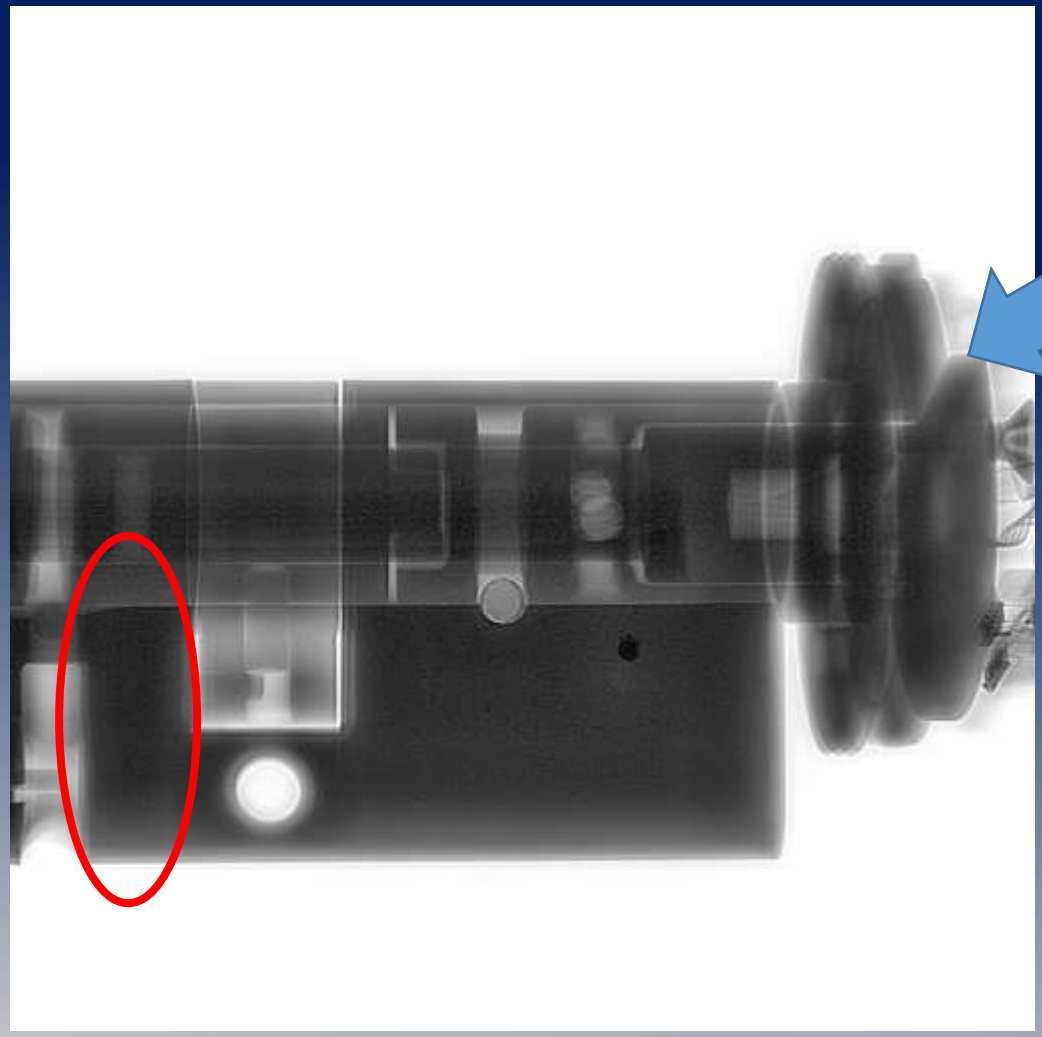


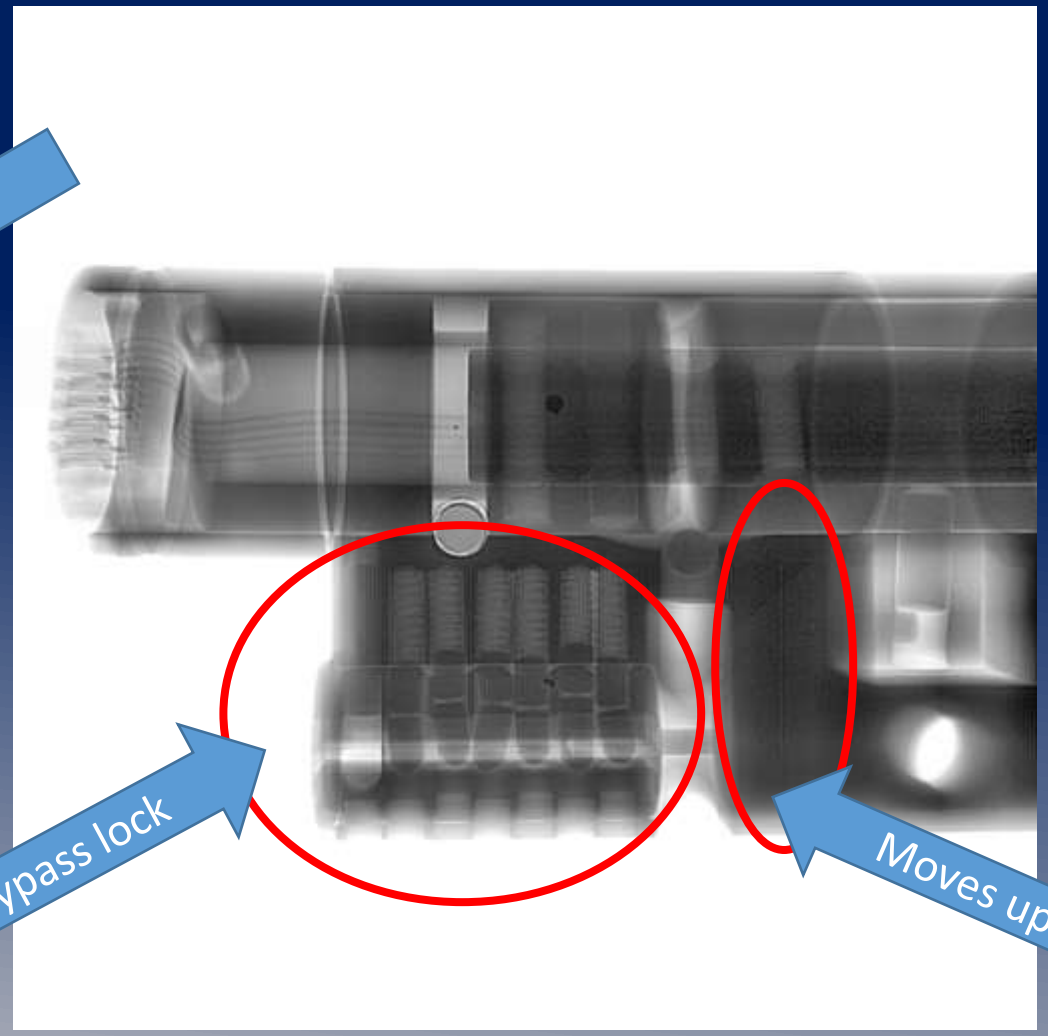
Unlocking with magnets and DC Motor



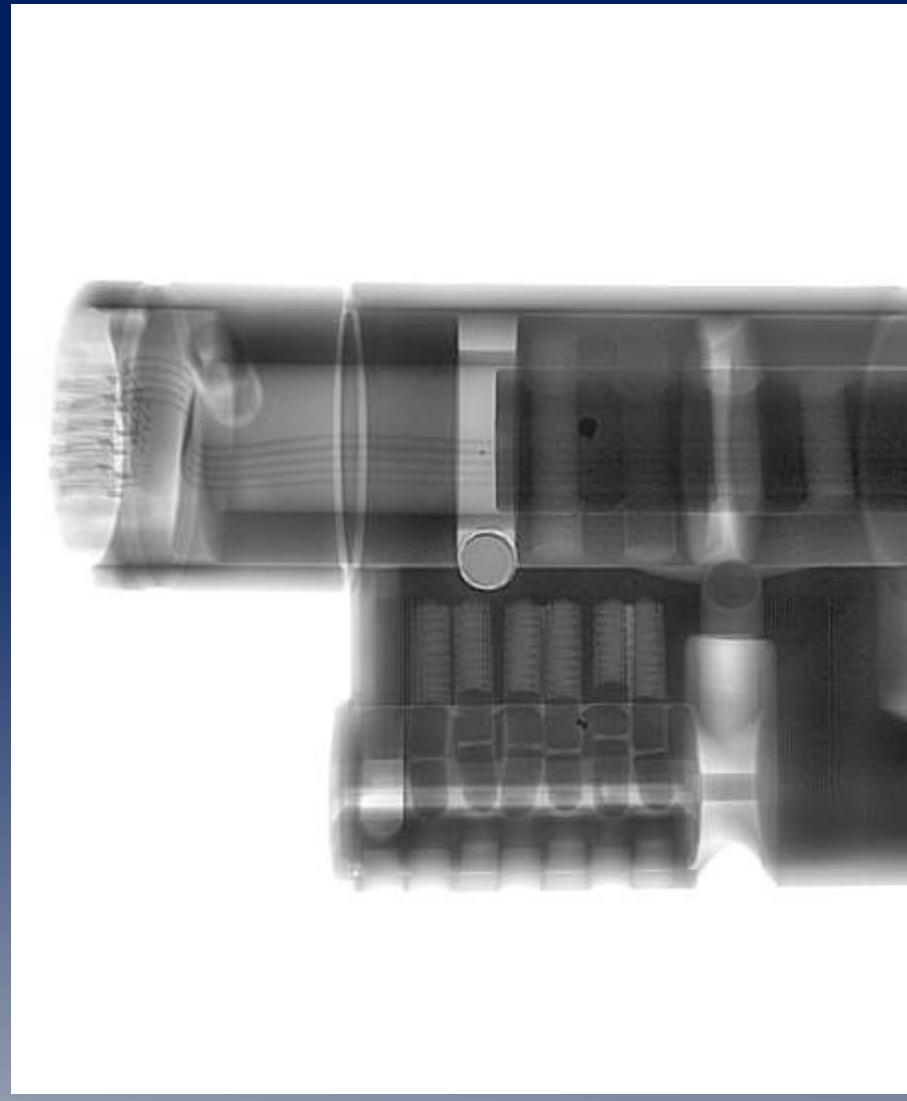


Unlocking with DC Motor and bypass lock





Sample of bypass or emergency key



Are smart locks secure?

Well, lets think about it later,
after learning more about attack vectors?

The attack vectors

Attack Vectors

I’m not using RFID, NFC, Bluetooth, WiFi or other for this type of attacks. These types of attacks are covered in other Talks

Only need access to the lock

- Think back to the outside and inside designs
- How to get access to the electronics

New technology = new attack vectors

	Mechanic locks	Electronic locks
# of issues	2	5

Compared to mechanical locks, multiple new attack vectors added

1. Transponder issues
2. Electronical issues
3. Electromechanical issues
4. Mechanical issues
5. Bluetooth / Infrared or WiFi

Batteriewechselschluessel

What you need to open the device and get a closer look

Where to get the Batteriewechselschluessel ?

You can by them on the Web

After cap removal

PCB

Battery

cables

antenna

Attack #1 - bypass

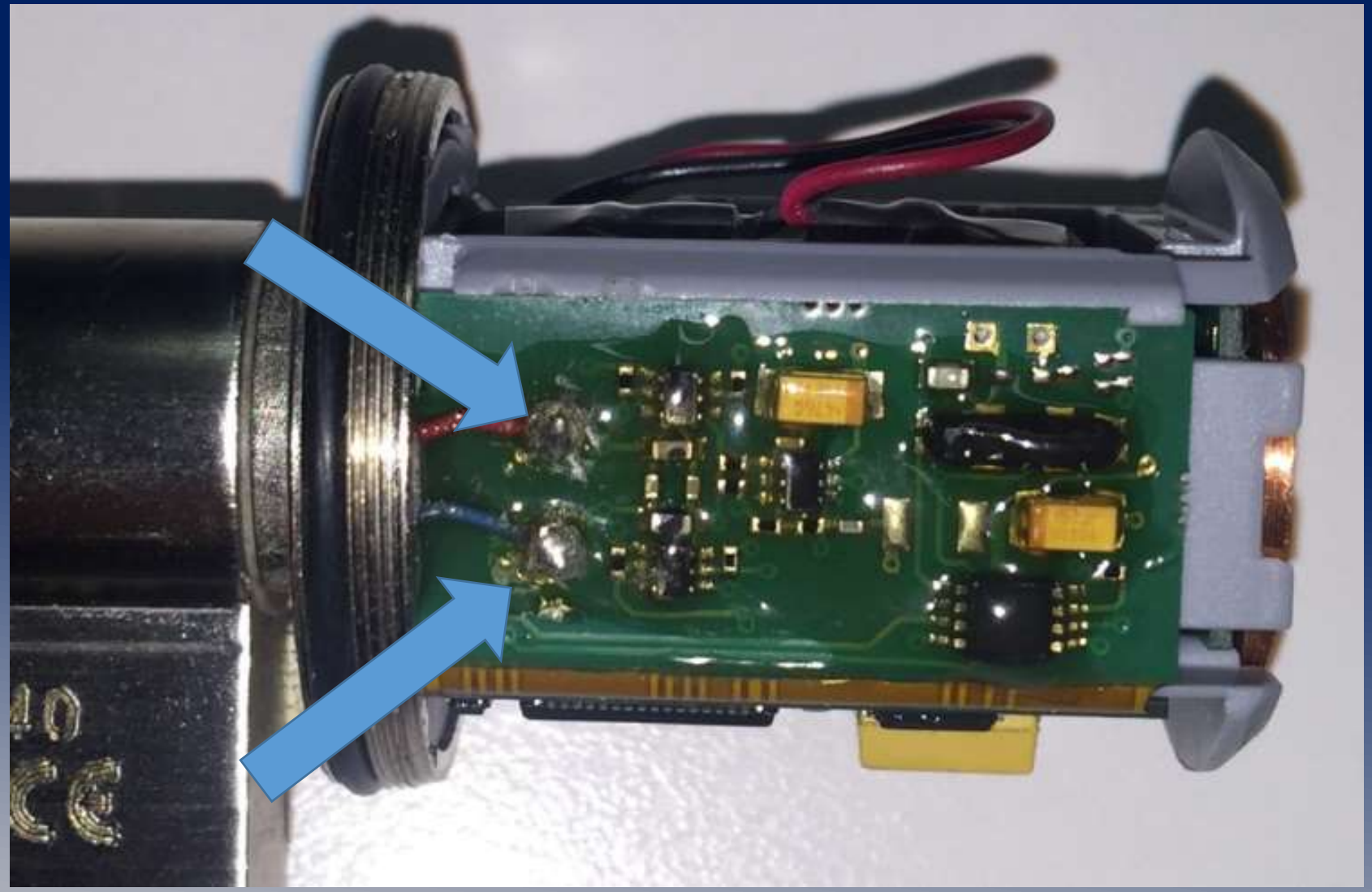
- Bypass the electronic
- Direct access the motor or coil

Attack #1 - bypass

Power source
for the
internal DC motor

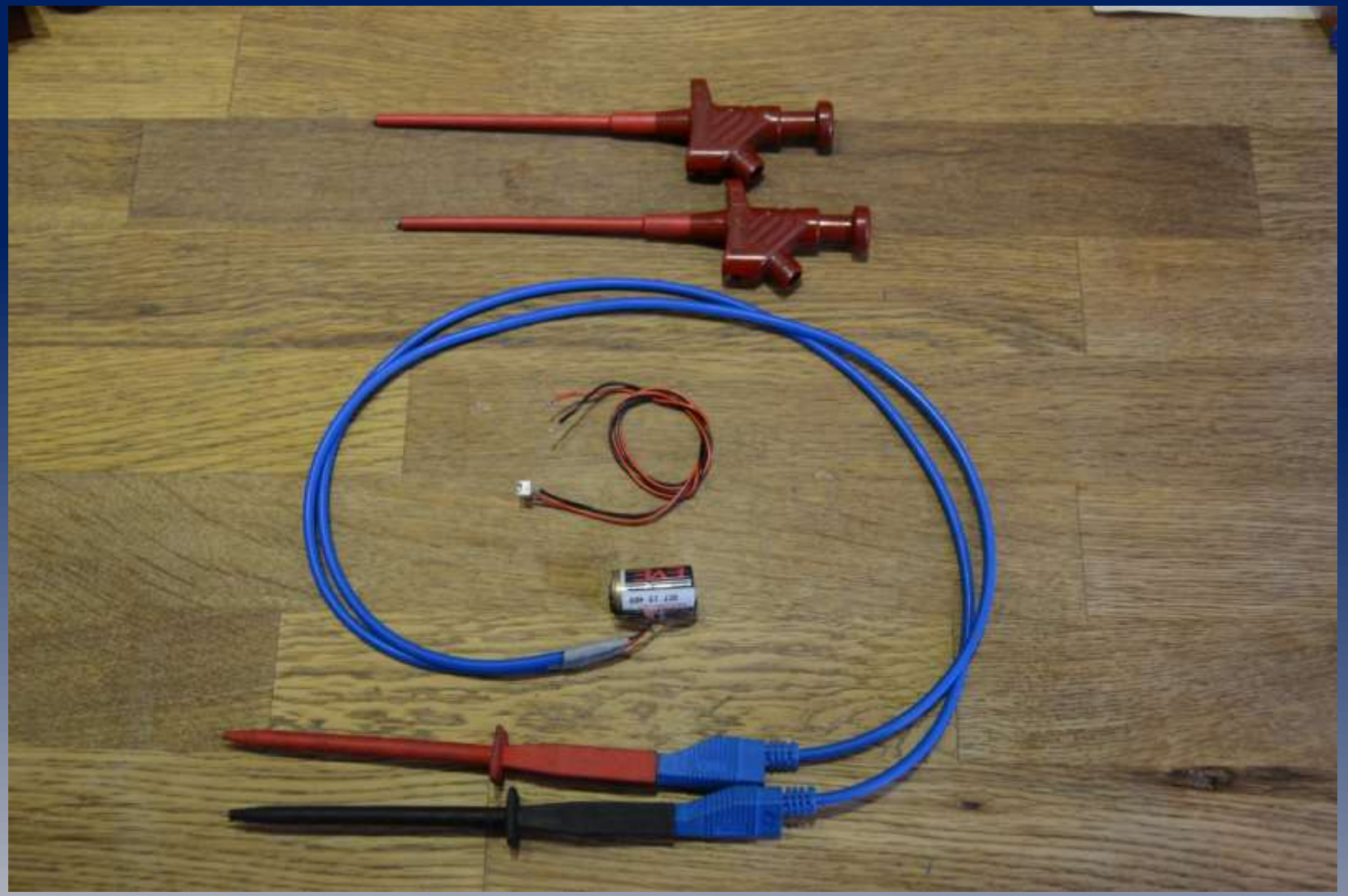
Controls
position of
the magnets

Remember:
On unsafe outside

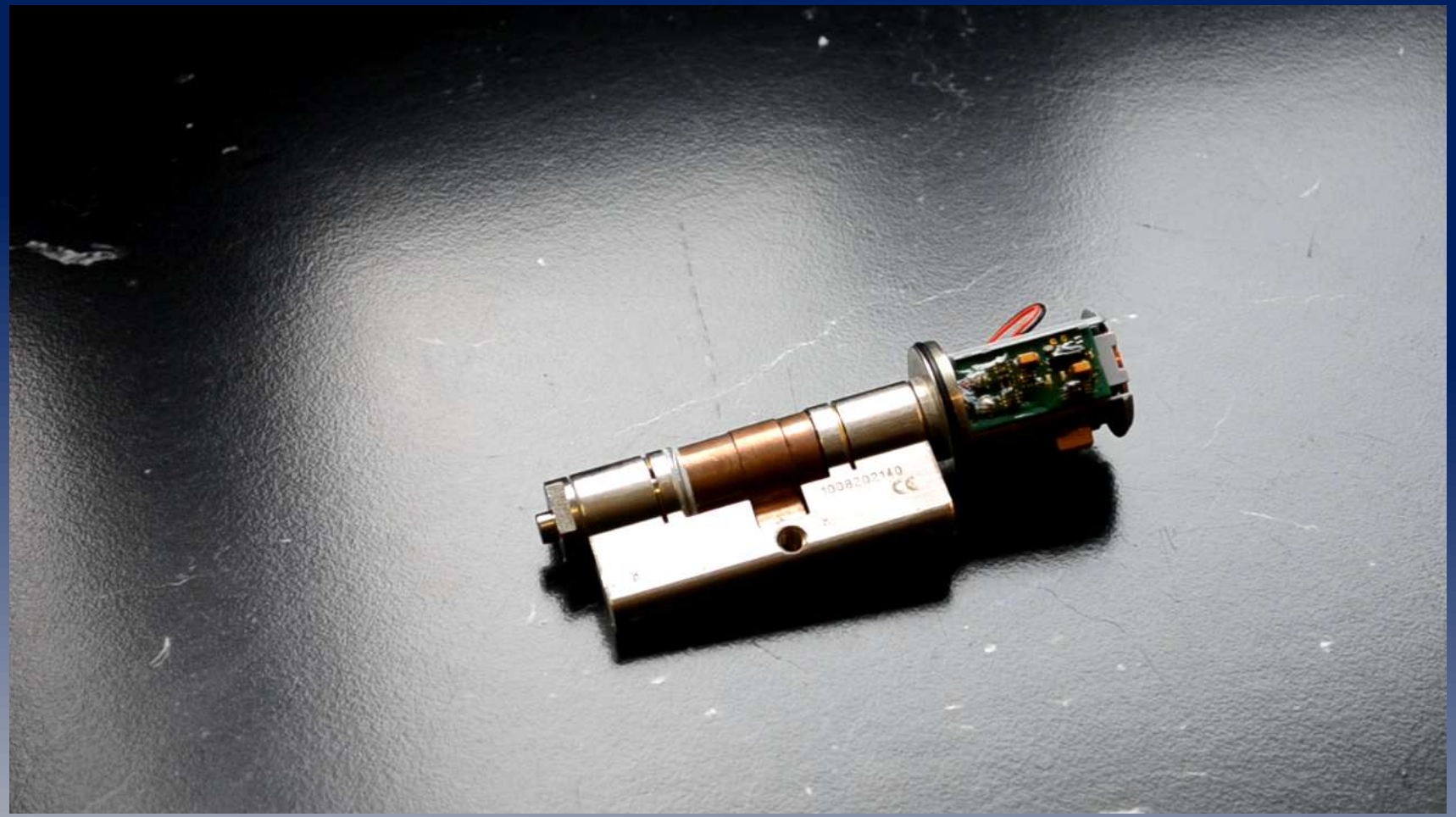


My weapons

- Battery 3.6 V
  (Oem spare Batt.)
- cable
- Measure tips

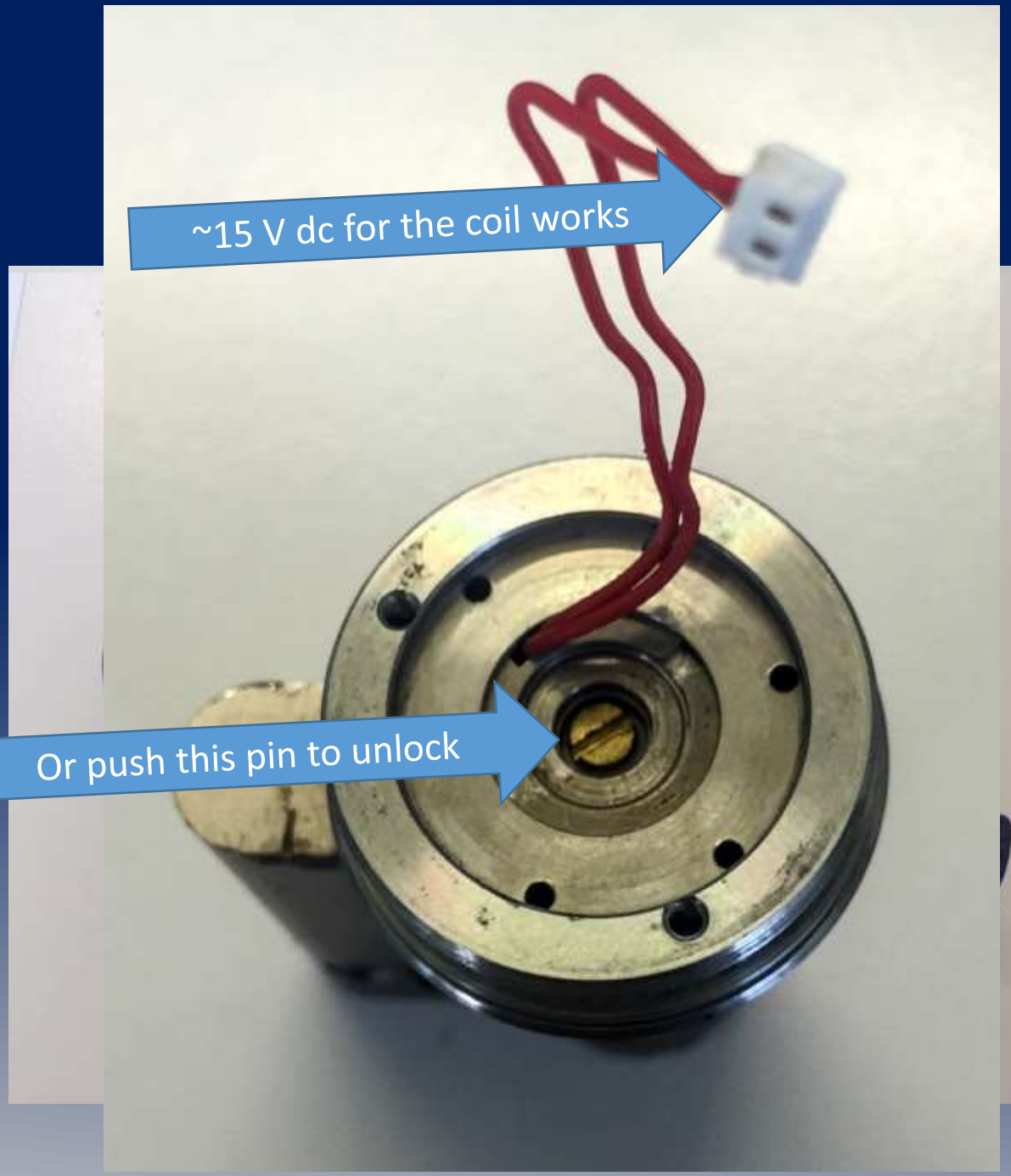


Demo



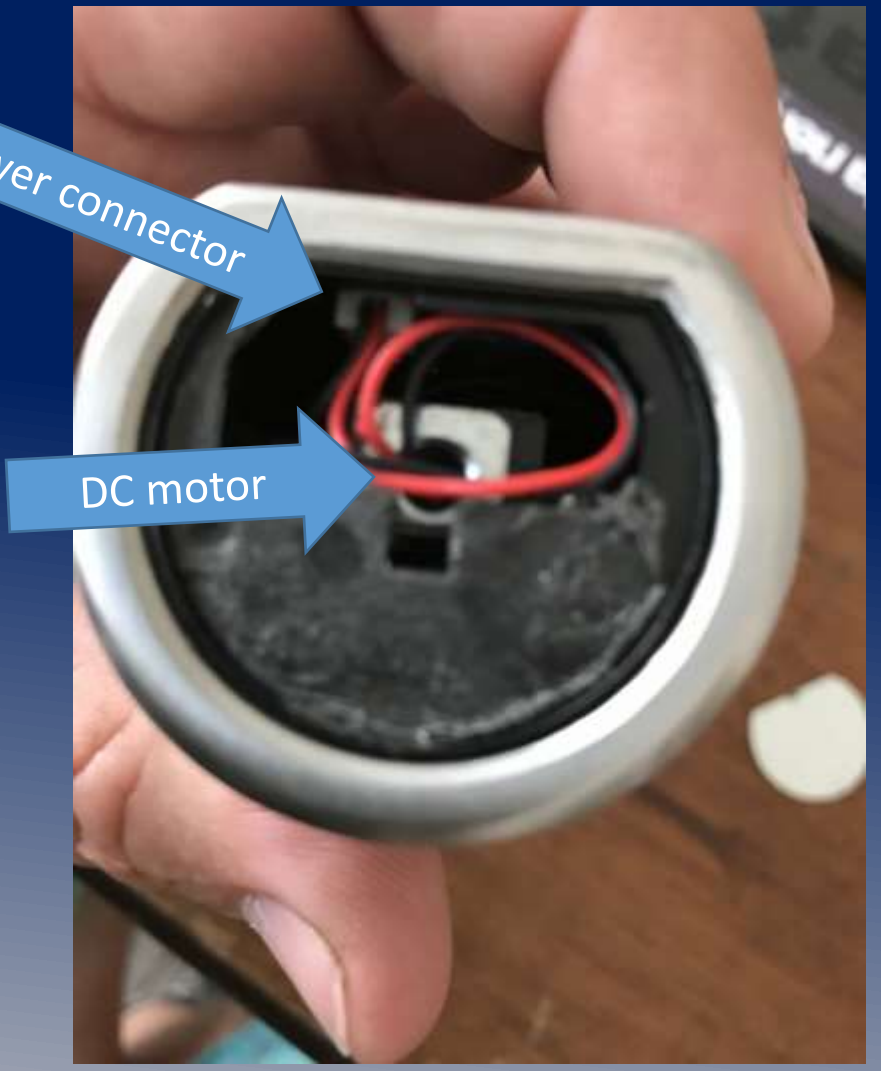
Half-cylinder

- Used in Fire preventing Doors,
- Glassdoors or other
- By design, all “outside”
- RFID electronic “outside”
- Electronic access to unlock
- This model has also a mechanical bypass



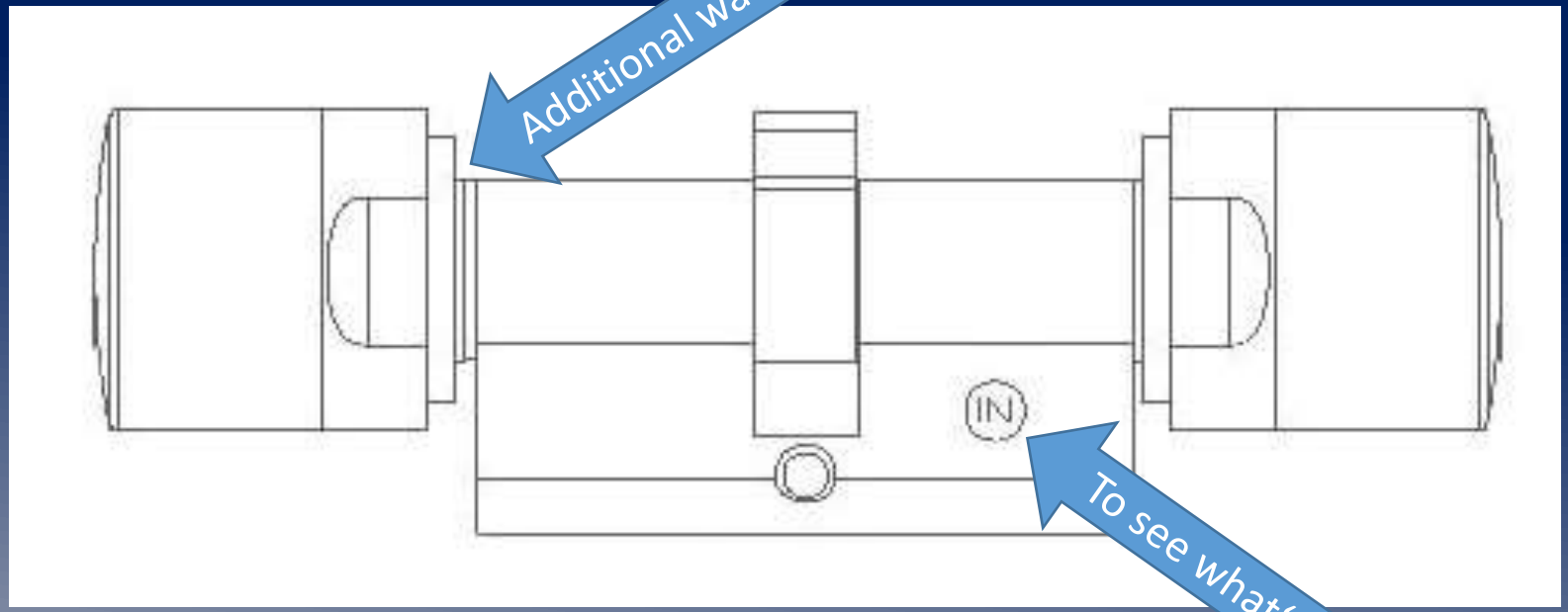
Attack #1 – bypass: some are very easy

- a knife needed to remove cap



Inside out mistakes could happen

Don’t assemble the inner sider out!



Inside out mistakes could happen

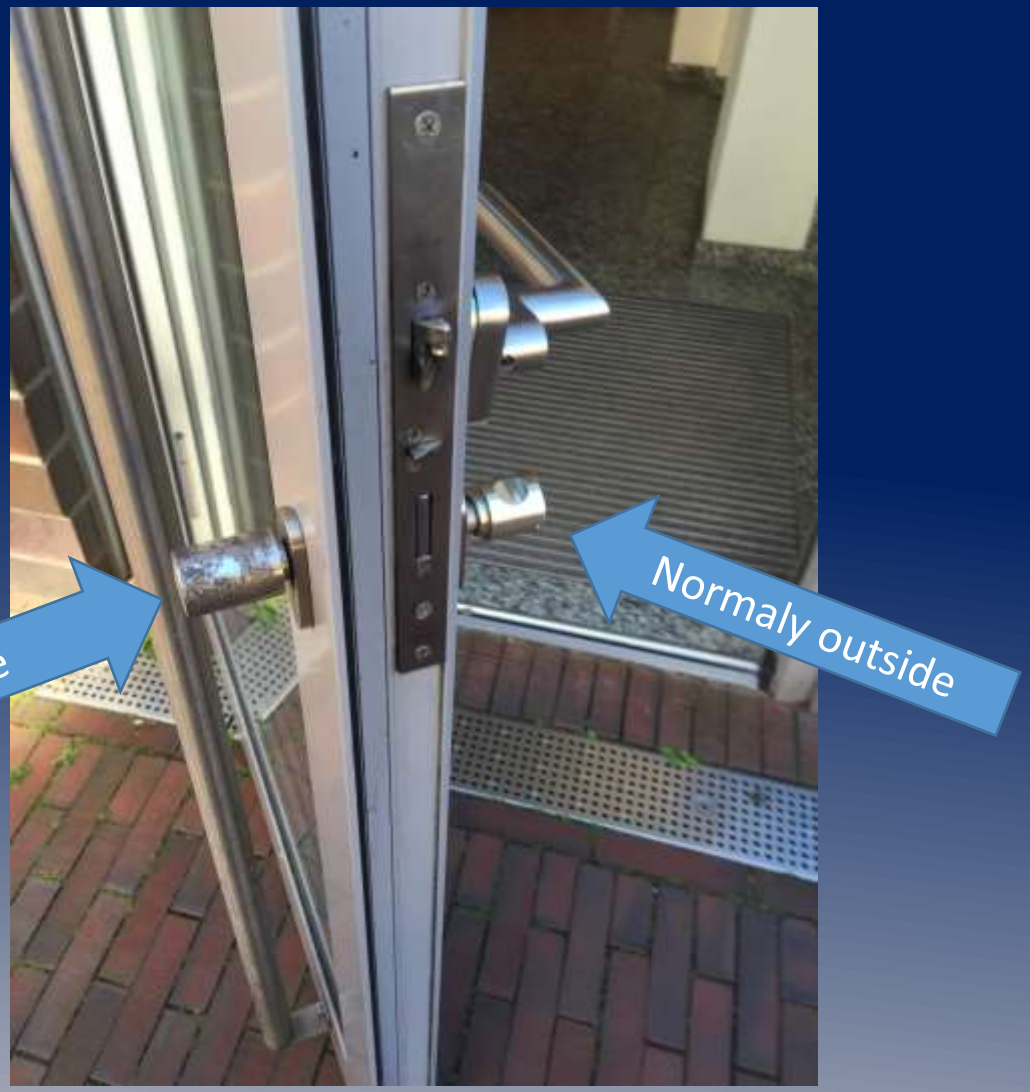
You think, this could not happen.

Wait…….

Emergency exit of a Bank

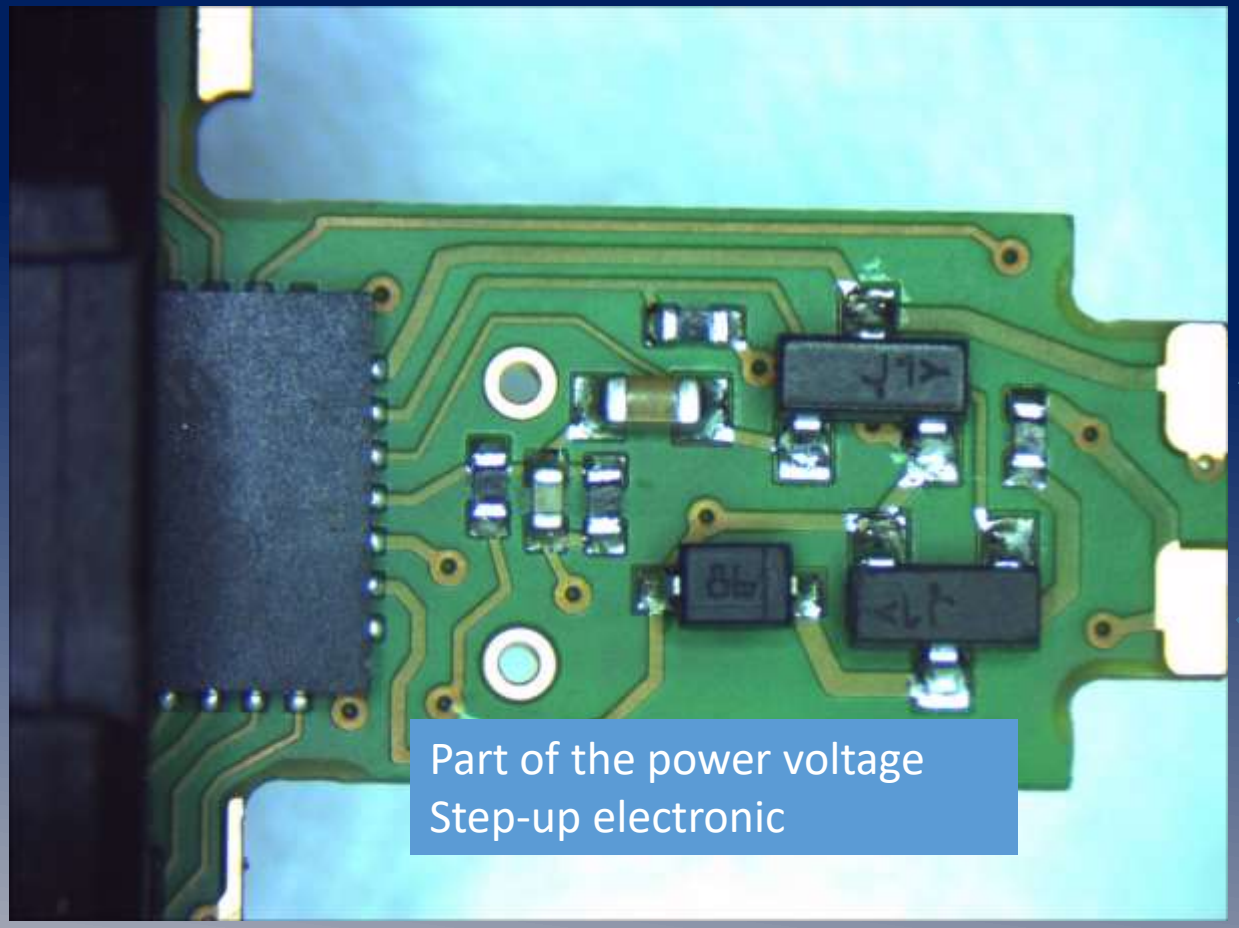
Vendor assembly instruction:
In emergency exit doors , the lock has to be mounted this way

They chose the wrong lock for this kind of door



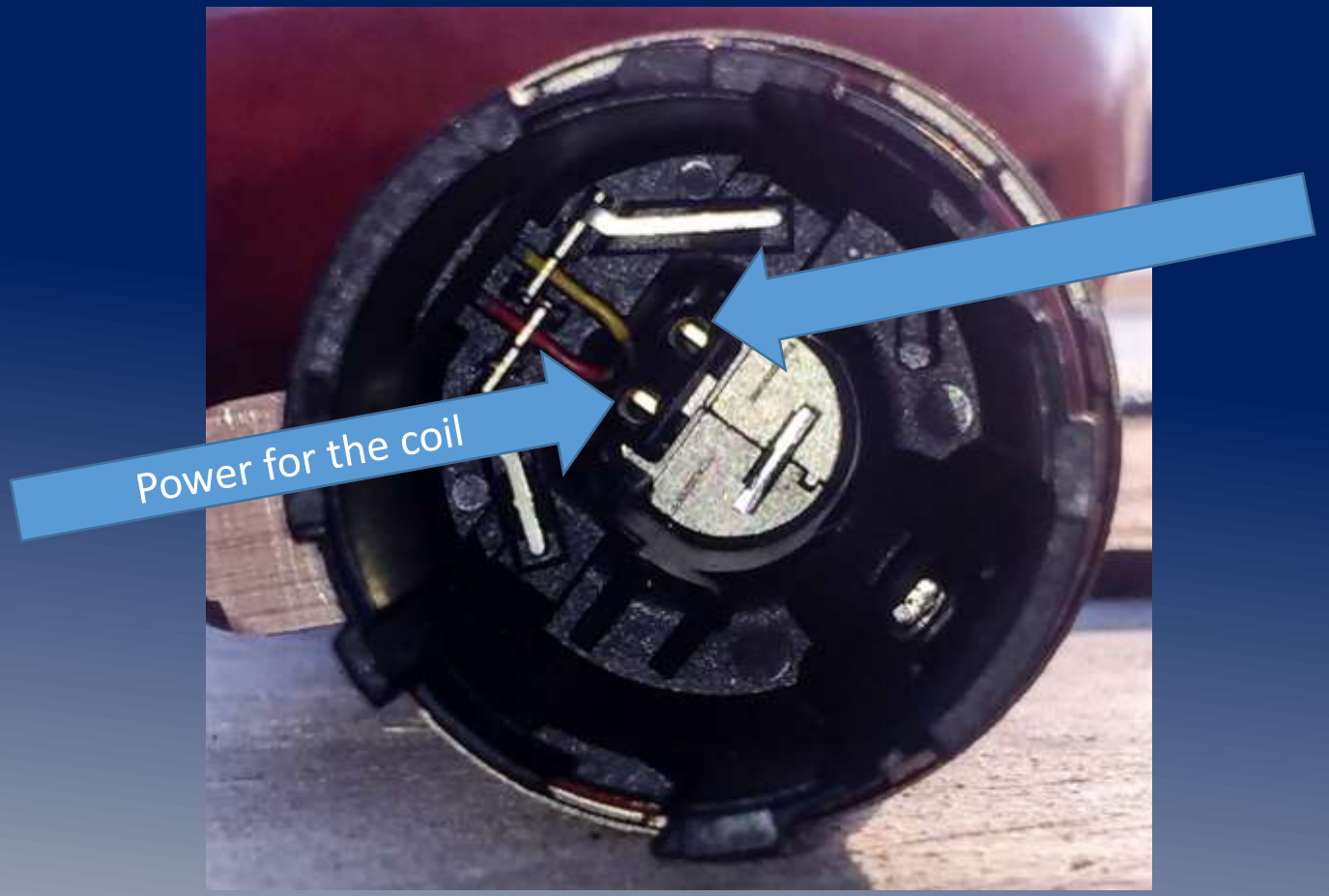
Attack #1 – bypass , on wrong mounted locks

POI - Point of interest on the PCB



Connectors to the internal coil

POI - Point of interest

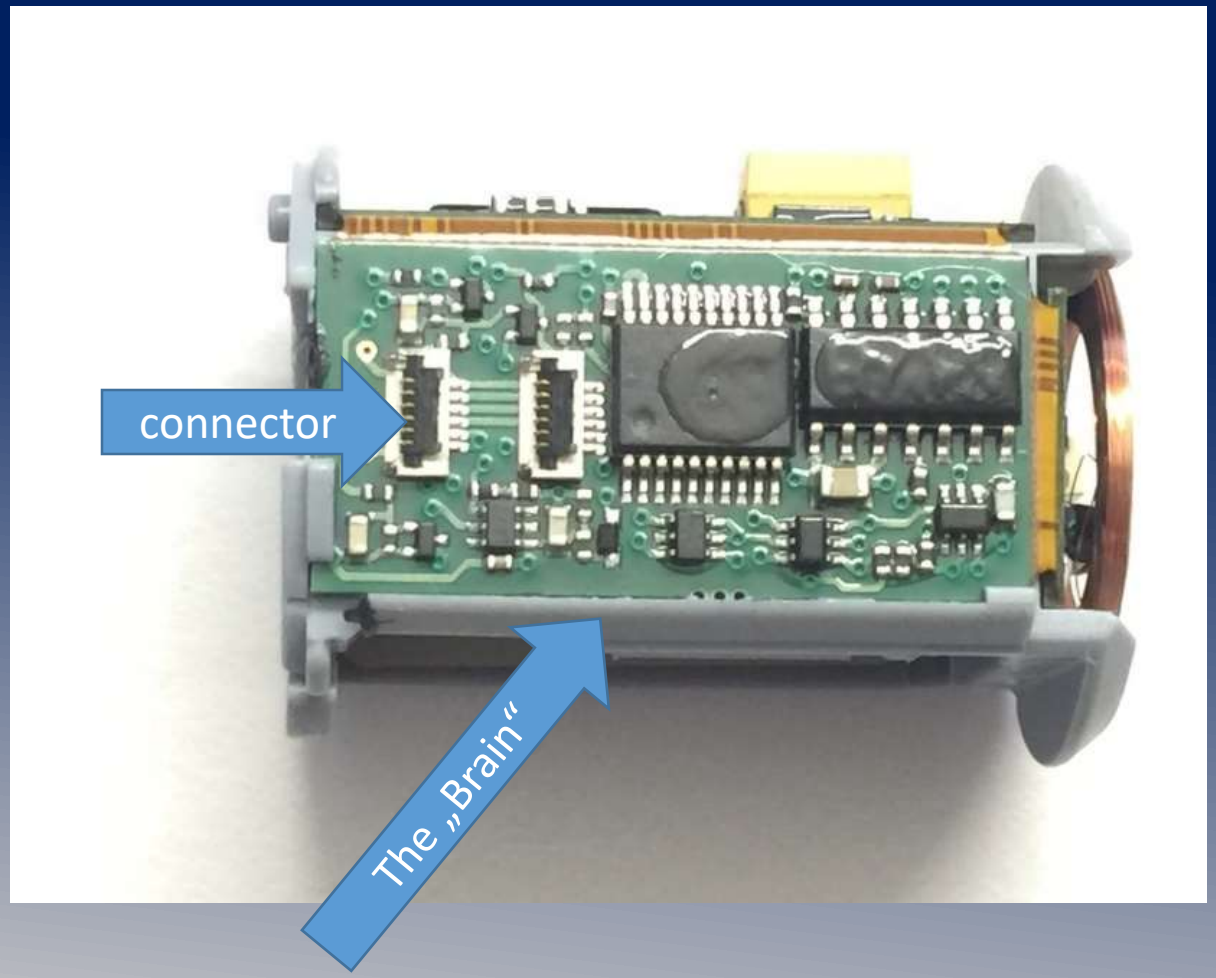


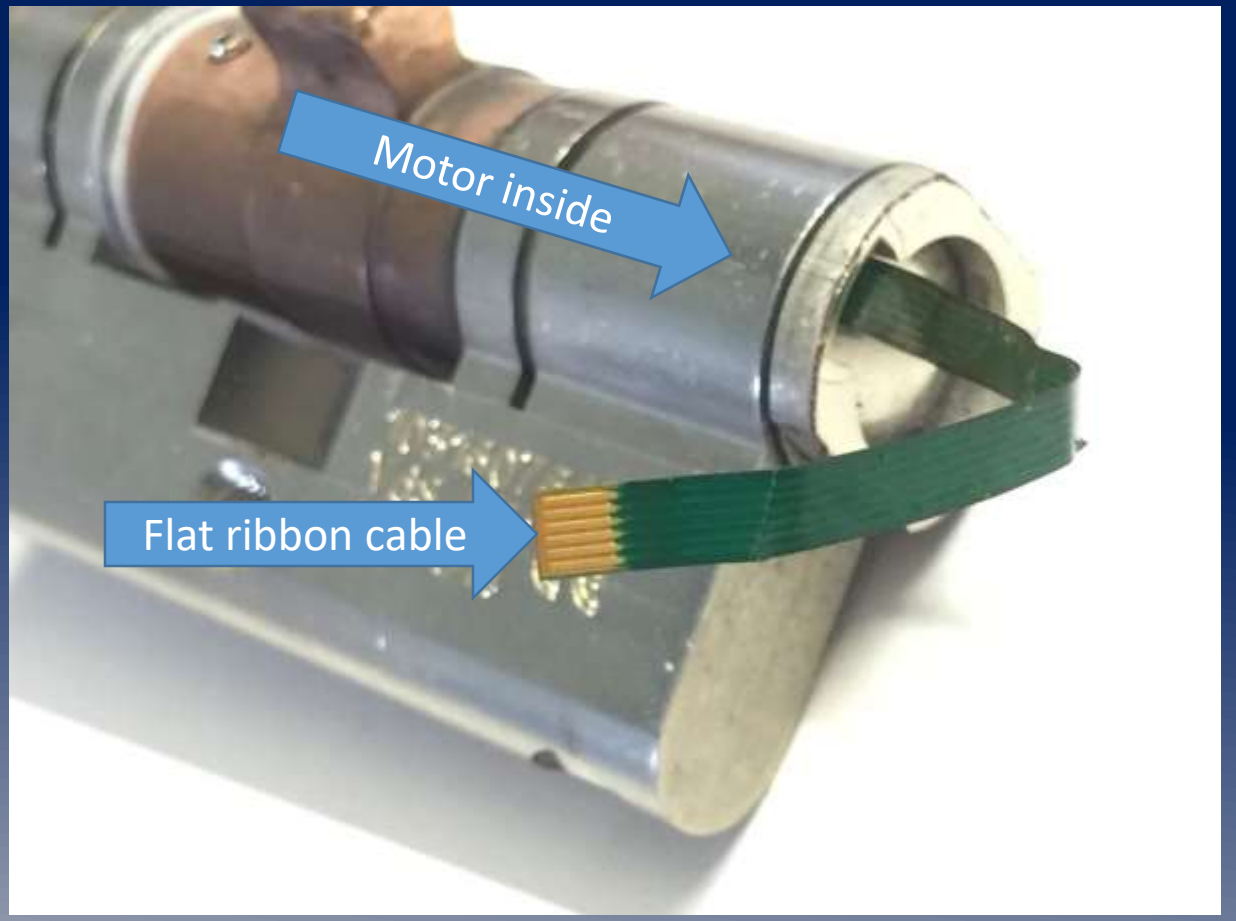
Insert cable
~15 DC unlocks

Attack #2 – signal replay

- Measure the signal on the wire
- Analyze the signal
- Replay the opening and closing sequences

Attack #2 – signal replay





NXP HTRC 110

NXP HTRC 110 Reader Chip

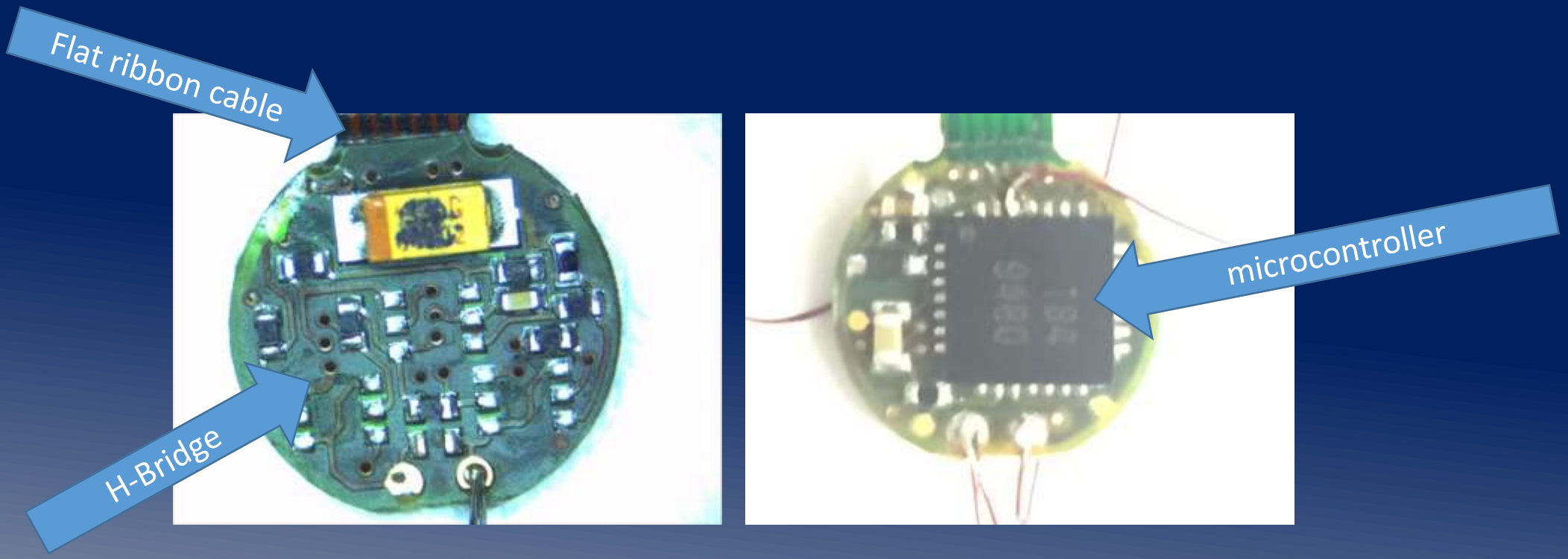
- very Low Power Stand by mode
- low external component count
- AM/PM Modulator (AM for write mode, AM/PM for read)
- On Chip Oscillator
- no memory

NXP HTRC 130

NXP HTRC 130 Co Processor

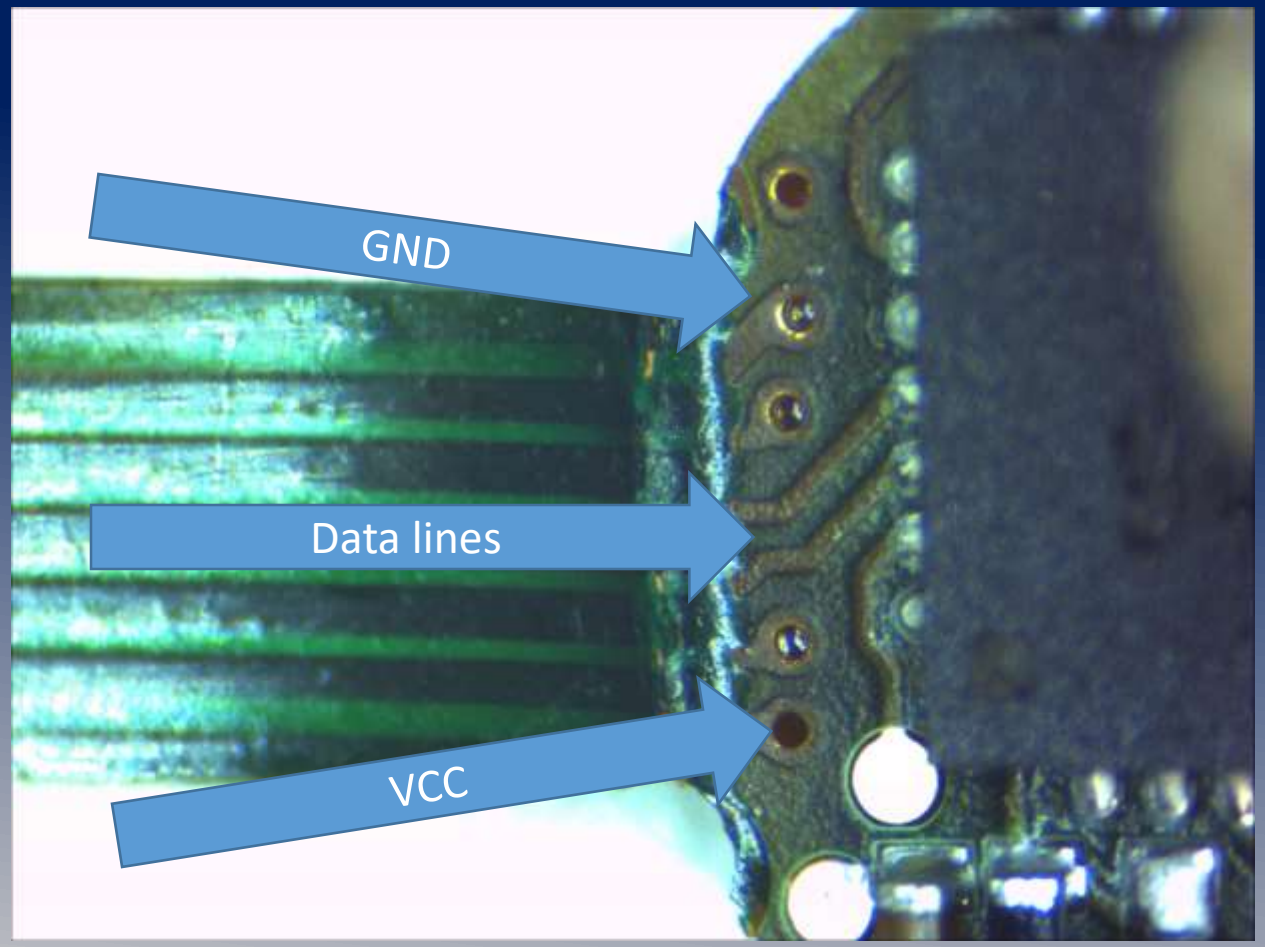
- data encryption
- mutual authentication
- password verification
- on-chip EEPROM to store secret data (but not used)
- uncomplicated host interface
- sleep mode for reduced current consumption

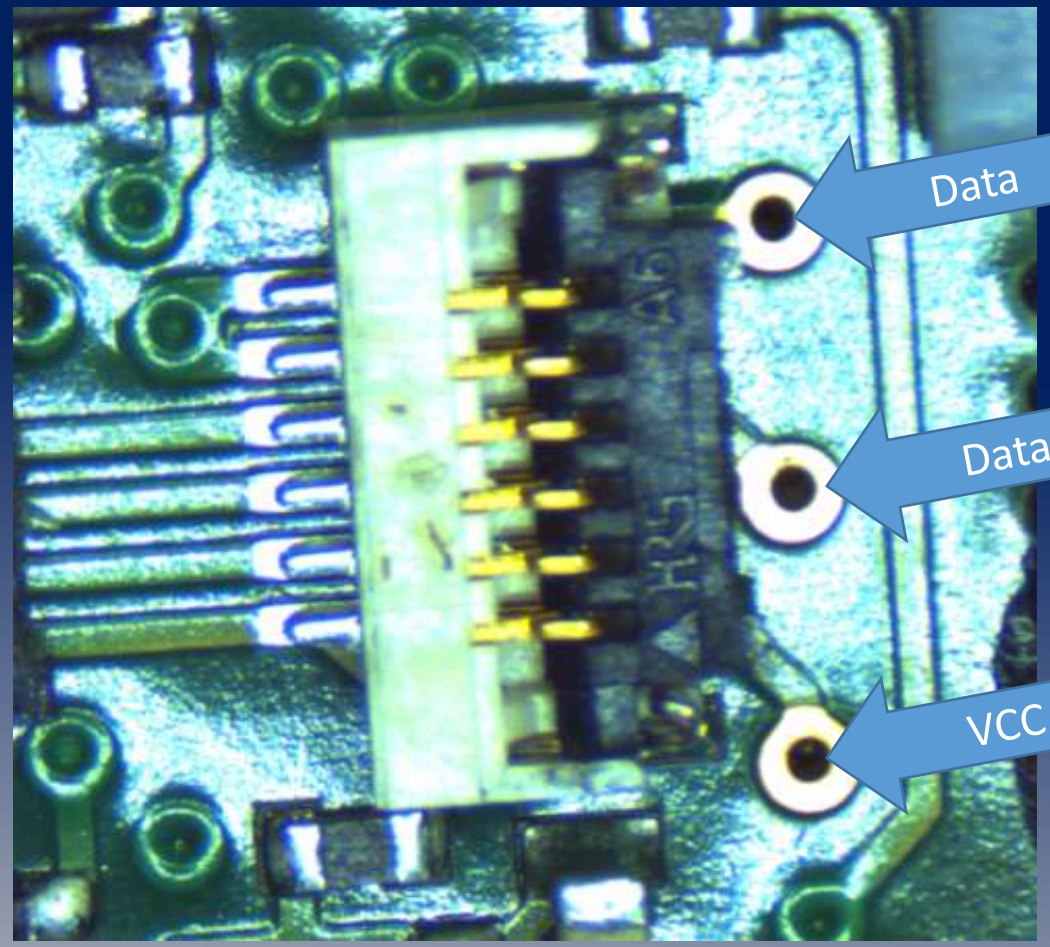
Motor electronics



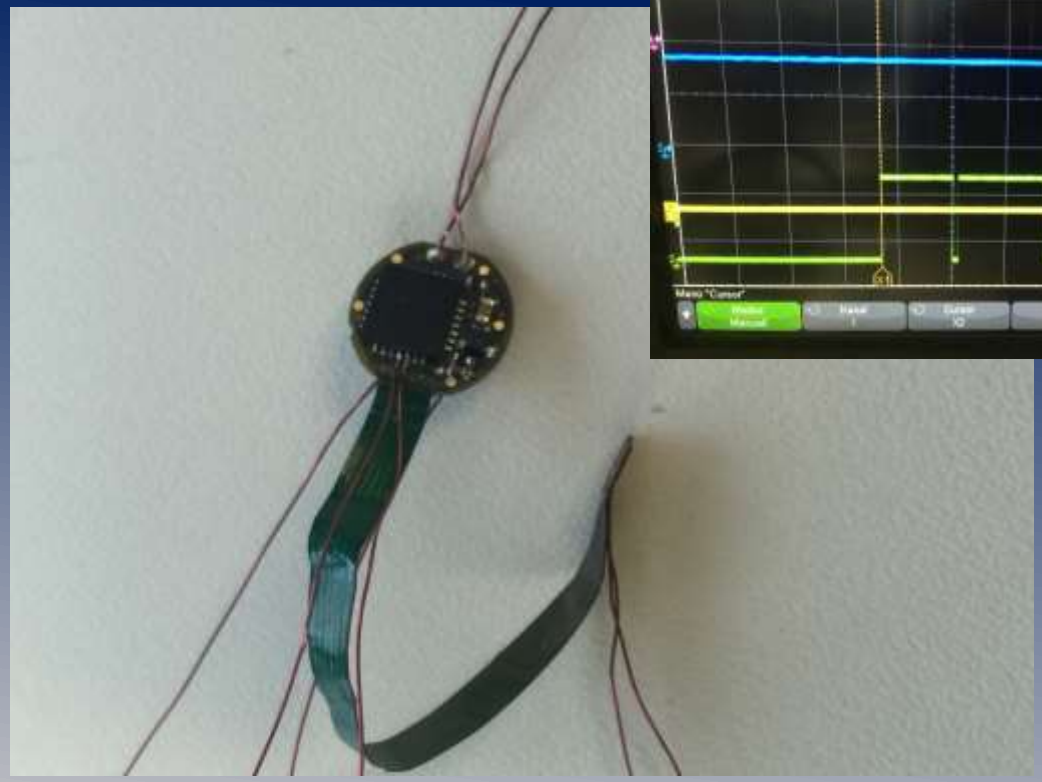
H-Bridge for left / right control of the DC Motor
PIC for “decoding” of commands
Communicates with the NXP HTRC 130 Co Prozessor

Where to measure

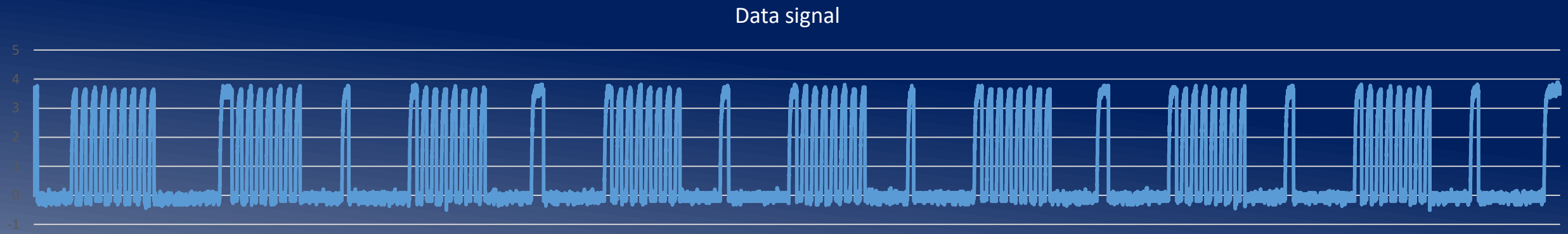




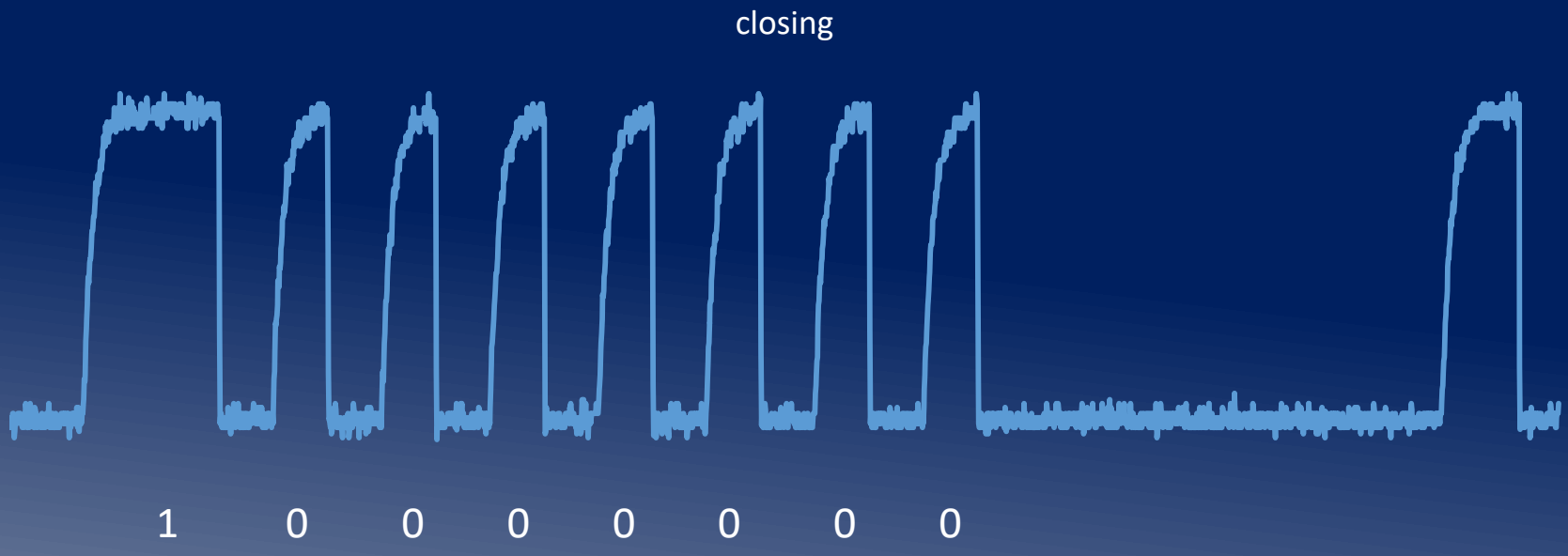
Analyzing the signals



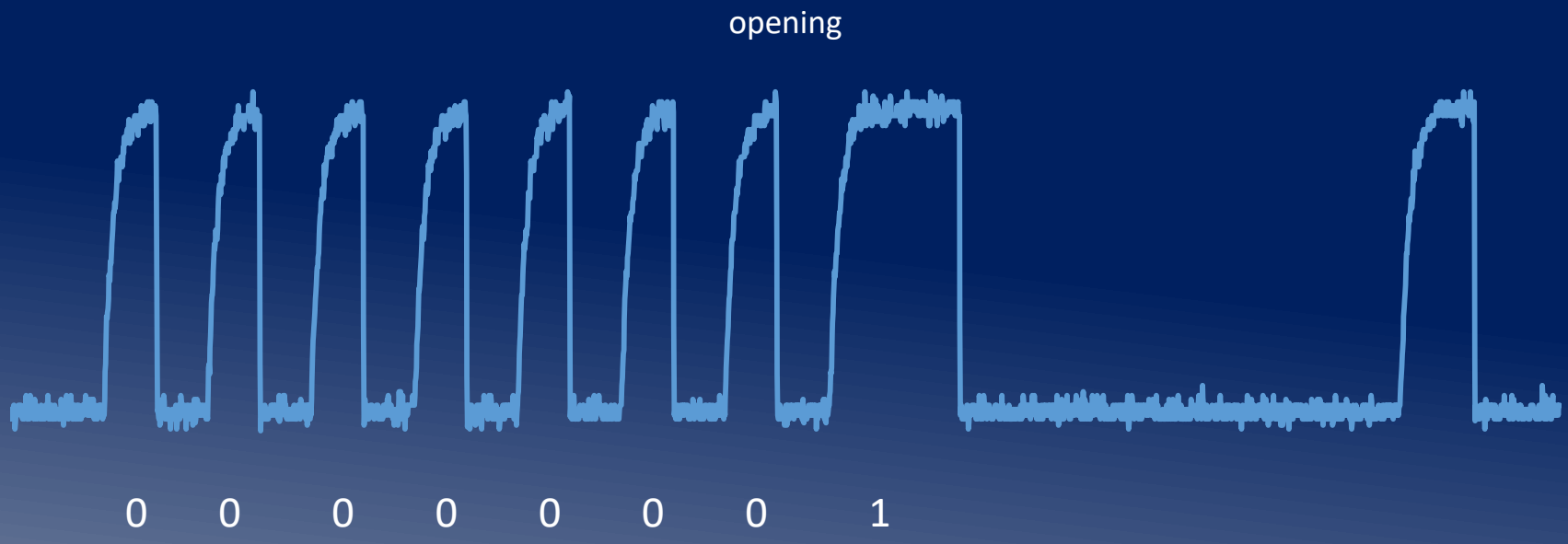
Recorded signal



Single Datagram for locking



Single Datagram unlocking



Failures implemented

Crypto co-processor not used

No authentication of motor PCB and main PCB

Plain serial protocol

Signal is reproducible

Lock is also vulnerable to “brain implant” attack

VDS certified locks

VDS BZ+ certified. What does this means

VDS = “Verband der Sachversicherer”

- “one of Germany’s leading independent testing institutions for fire protection & security”
- VDS certified Products must comply with several requirements
- Written down in DIN Norms

BZ+ = extra protection against Drilling and pulling of the cylinder

- Stands for extra mechanical protection

But....

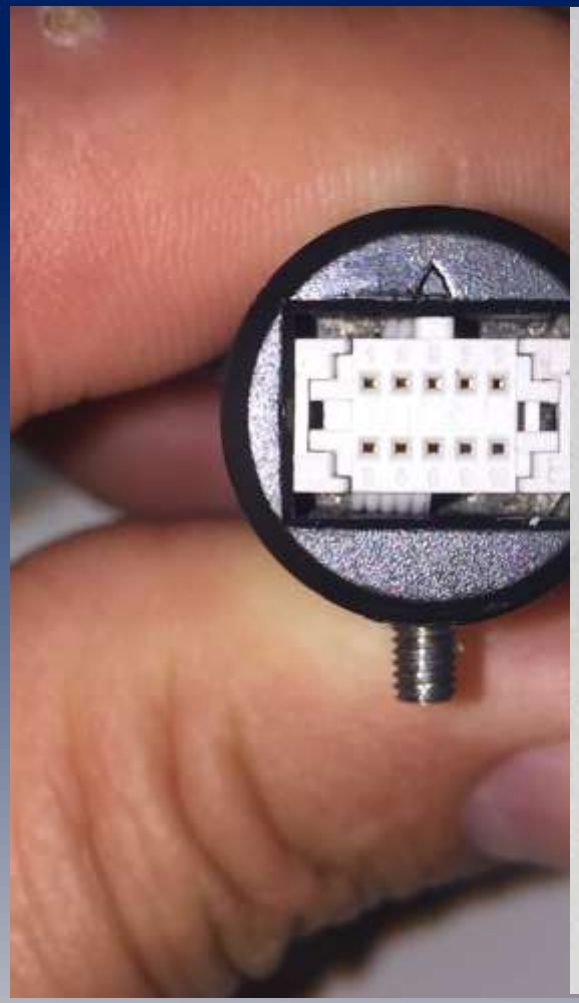
VDS certified does not mean that these locks are secure.

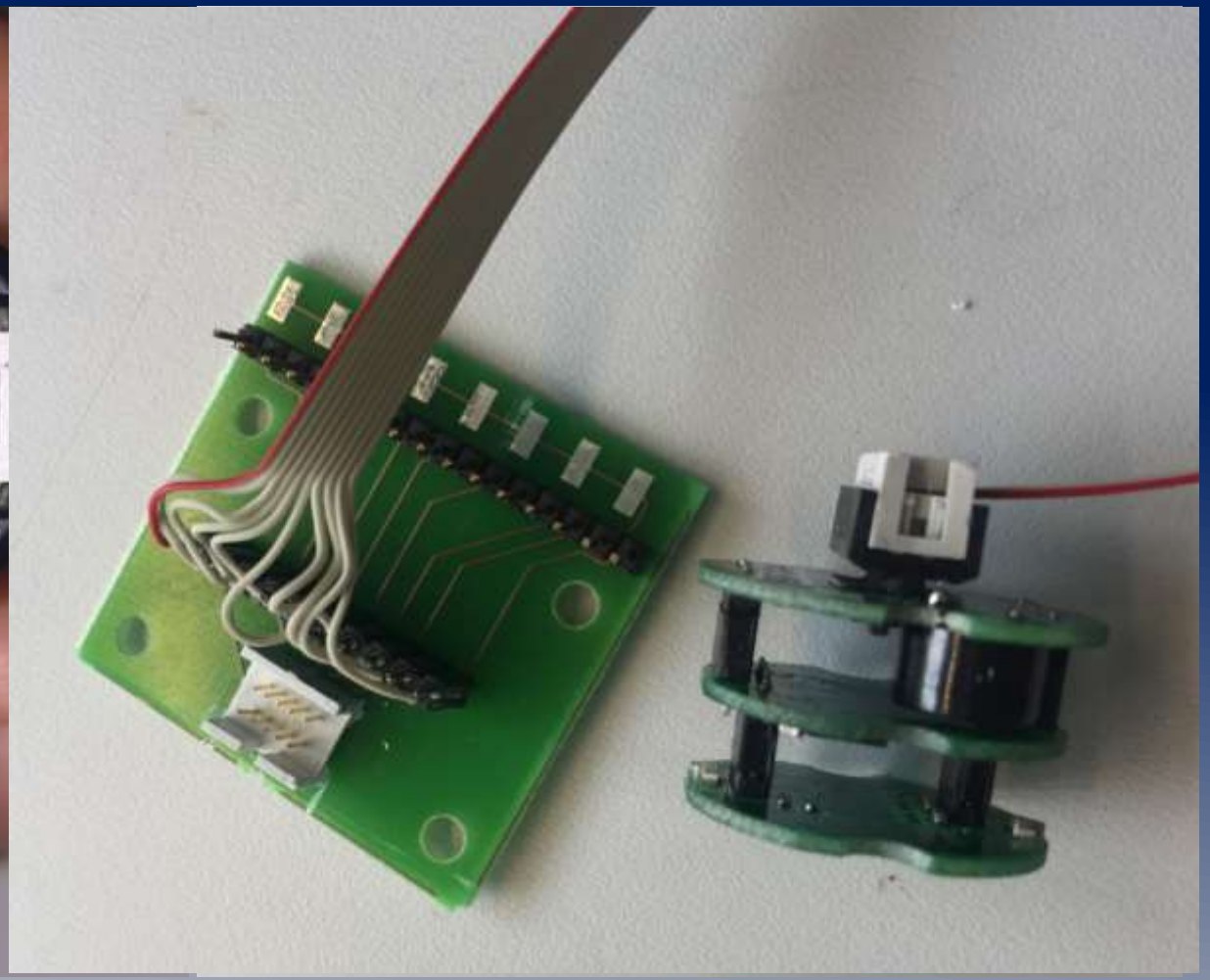
Currently, the VDS testing DIN does not focus on details of the smart locks

far as I know, these parts are not in the test specification :

- Encryption of transmitted signal
- Authentication of electronic parts
- Code audits of the firmware (remember the RNG failure)

Attack #2 – signal replay, different lock



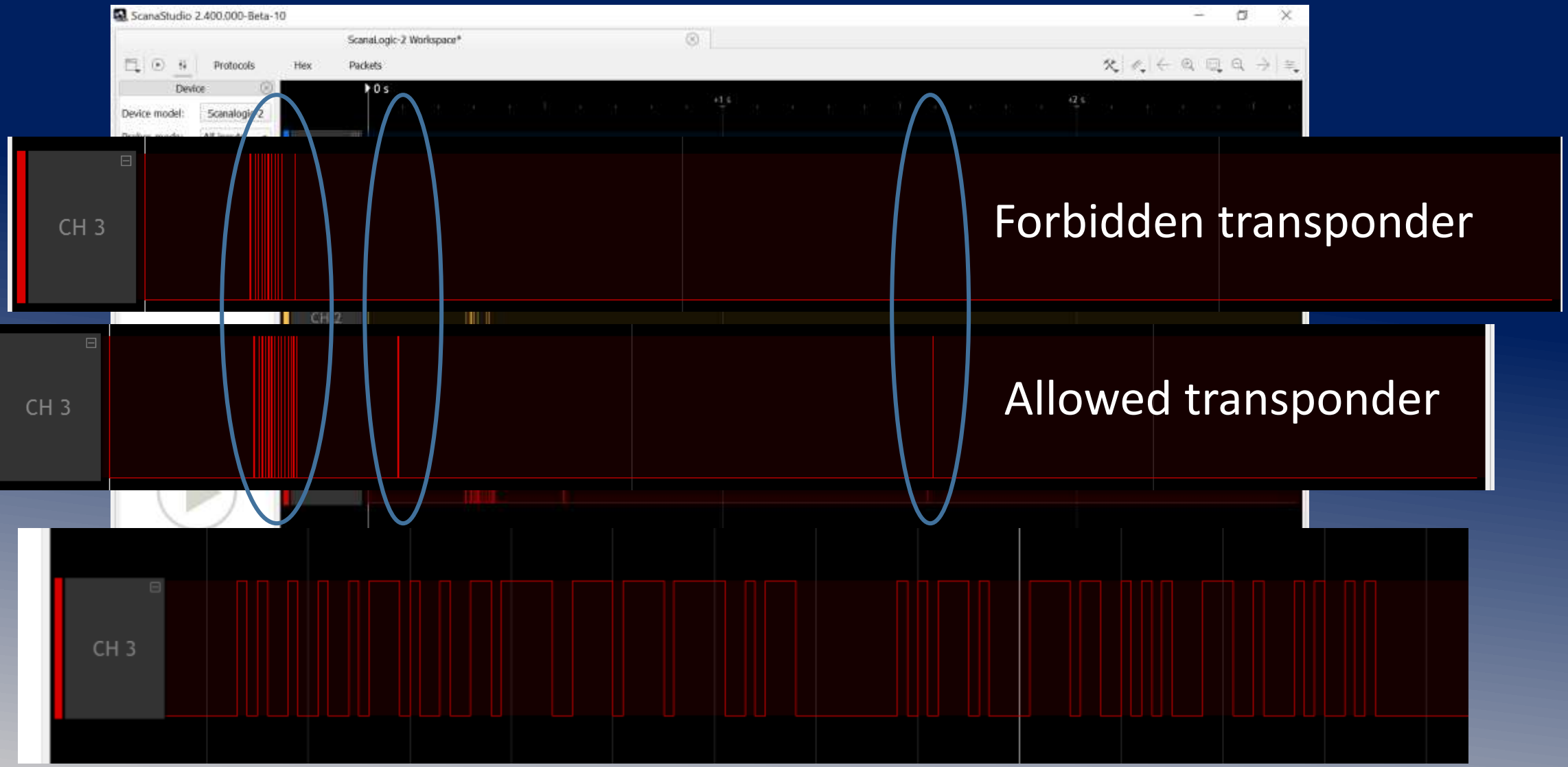


Attack #2 – signal replay, different lock

Logic analyzer for

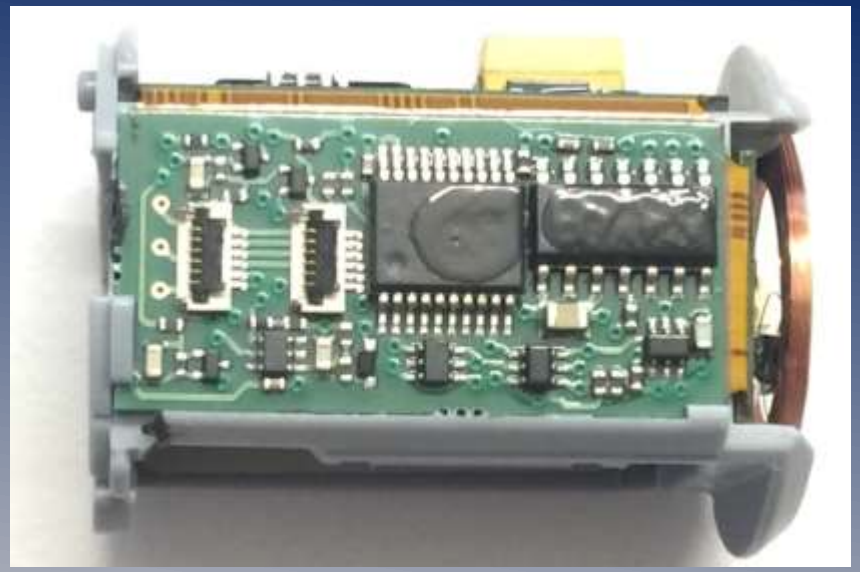
Signal recording

Measuring the signal



Attack #3 – brain implant attack

- Electronic needs to be outside
- Buy same lock
- Program with your Access Cards
- Temporarily replace the „brain“ with your electronic



Attack #4 – traditional lockpicking

Remember the bypass key

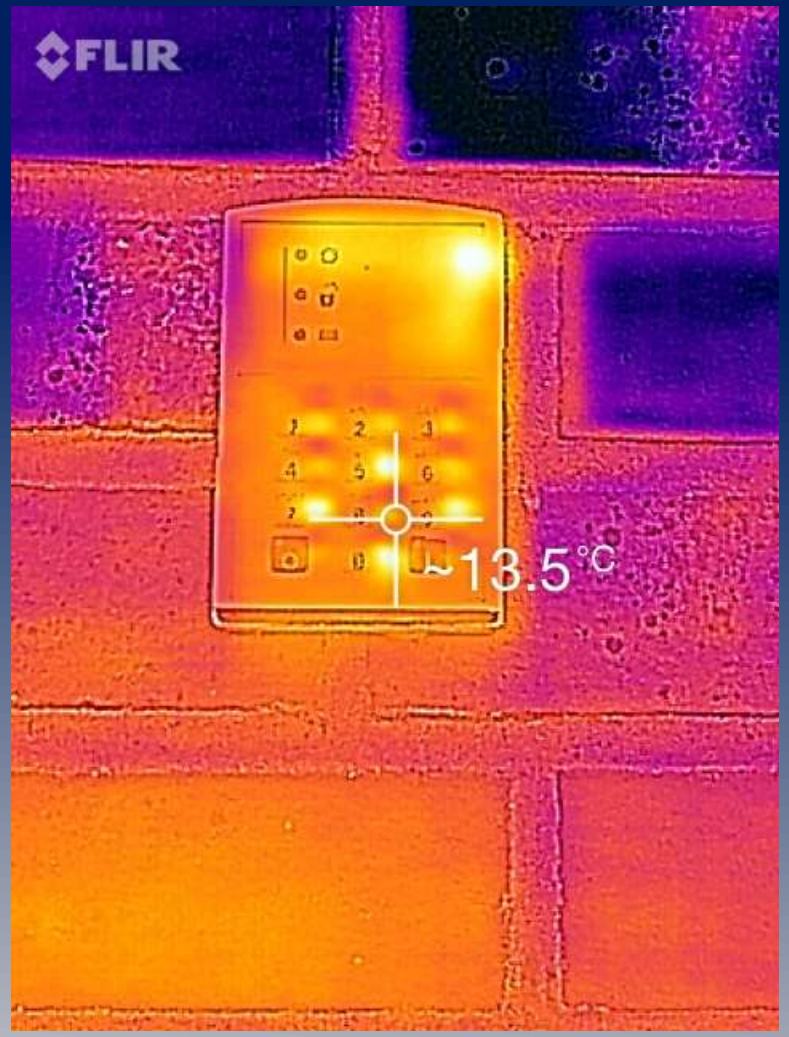
implemented to

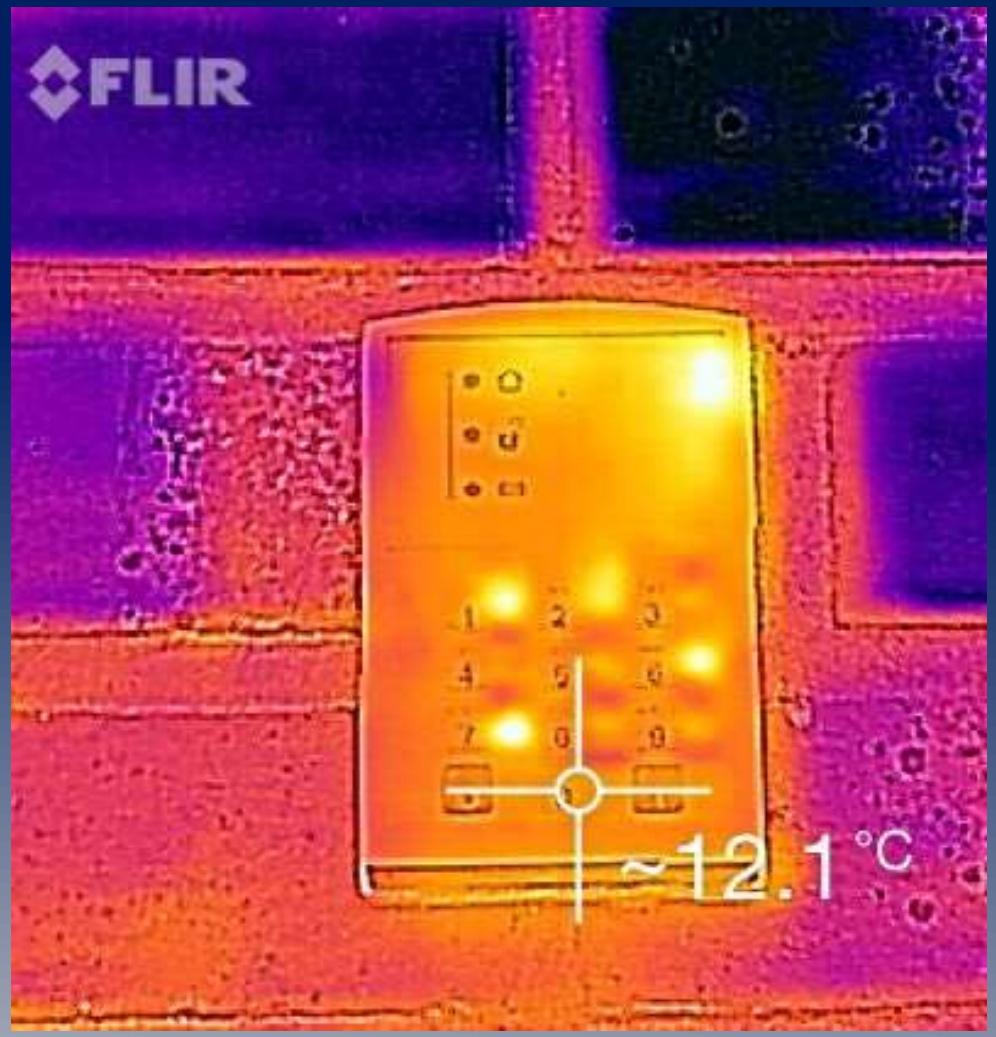
- bypass low battery
- Lost card or electronic error
- Other reasons i don‘t know

Attack #5 – other possible types

- Accu drill the knob until it opens
- I heard about a teaser attack https://www.youtube.com/watch?v=Zxj_2JI-F_U
- Bumping the lock
- Thermalimaging (think about if this is part of 2FA)

Attacking with thermal imaging





What we can do

Take a closer look on how vendors have build their locks

Define security zones and use the right locks for it.

Prefere those, where the electronic is on the inner sider

Choose a not broken Transponder type

Only a few exceptions allowed (see half cylinder)

A secure lock

Transponder electronics on “secure inner side”

Or, encrypted & authenticated communication between out/in

Transponder Type not on the broken Tags table

Mechanical design with no bypass

Assembled in the right direction

Some vendors started to secure the removal of the cap by Bluetooth!

Is a smart lock/ digital cylinder secure?

Well, it s up to you

follow the guideline from the previous slide

Be skeptical with new Smart Lock vendors, they promise much

Even vulnerable locks could be useful for some scenarios!

I personally prefer a different implementations of smart locks

fails


Steve Ragan @SteveD3 · 11 Std
But when audited, the company can honestly claim they've installed locks, and the gate uses a heavy chain.
148
156


1
2
3
4
5
6
7
8
9
0
#

Thank you for your attention

May the force be with u

@ObiWan666
info@ROSEN-DBS.com