Open sesame - or how secure is your stuff in electronic lockers

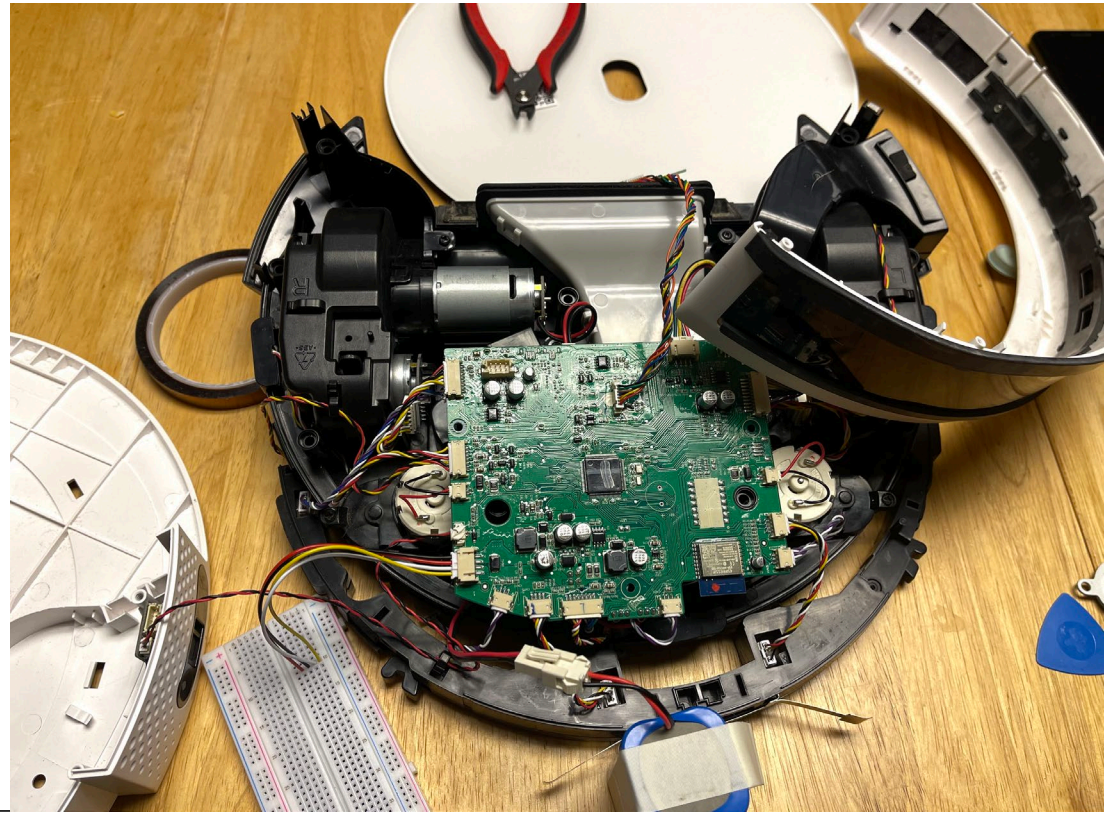
DEFCON 32 – Dennis Giese, braelynn

About Dennis

- “Security Researcher” aka Hardware Hacker
  - Research field: Wireless and embedded Security&Privacy
- Interests: Reverse engineering of interesting devices
- Vacuum Robot (and IoT) collector
  - Rooting of vacuum robots
  - https://robotinfo.dev
- Target of a “Cease&Desist”@DEFCON
  - (withdrawn as of 10.08.2024)

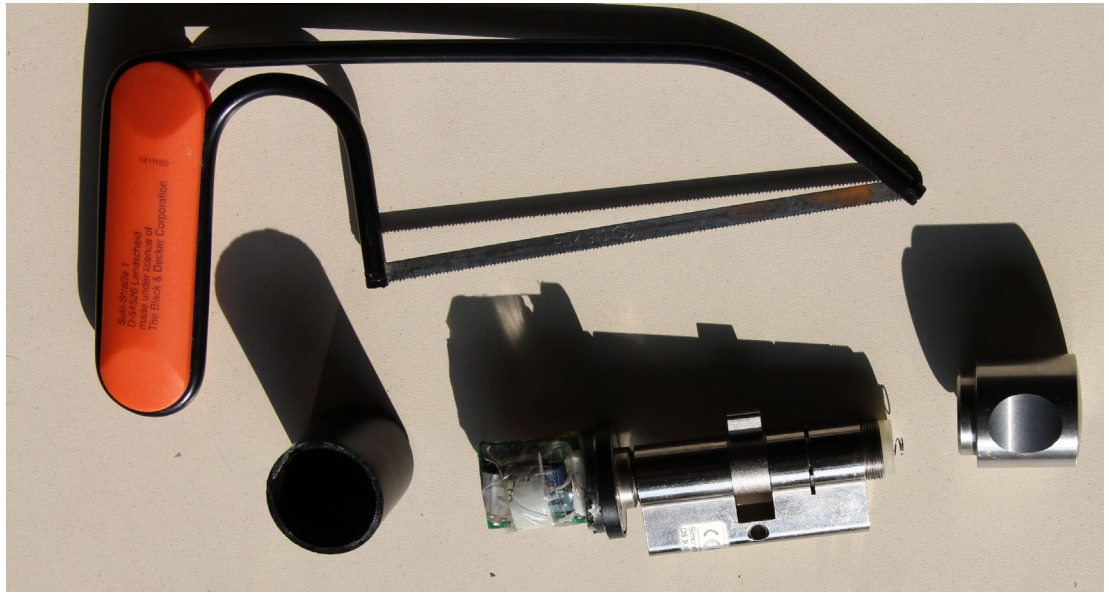
About braelynn

- Hacks things for Leviathan Security Group
  - (this talk is entirely personal research and does not reflect their views ;))
- Focus: Application Security and APIs
- Hardware hacking for fun
  - Robots, Cameras, Locks
- My first DEF CON talk
  - Also named in the Cease and Desist!

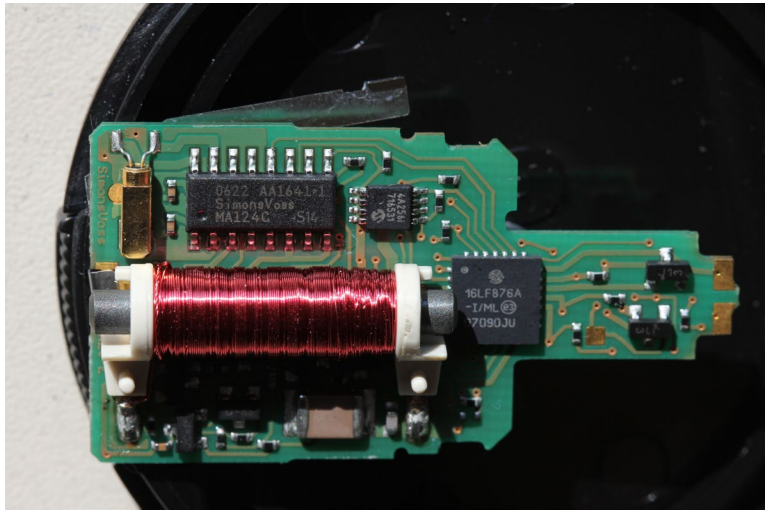


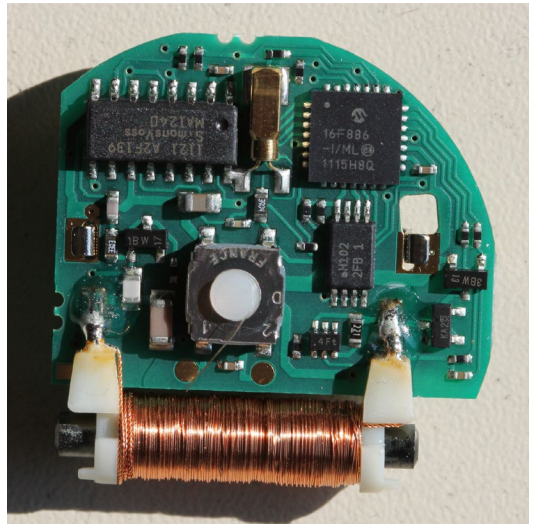
Previous work on locks

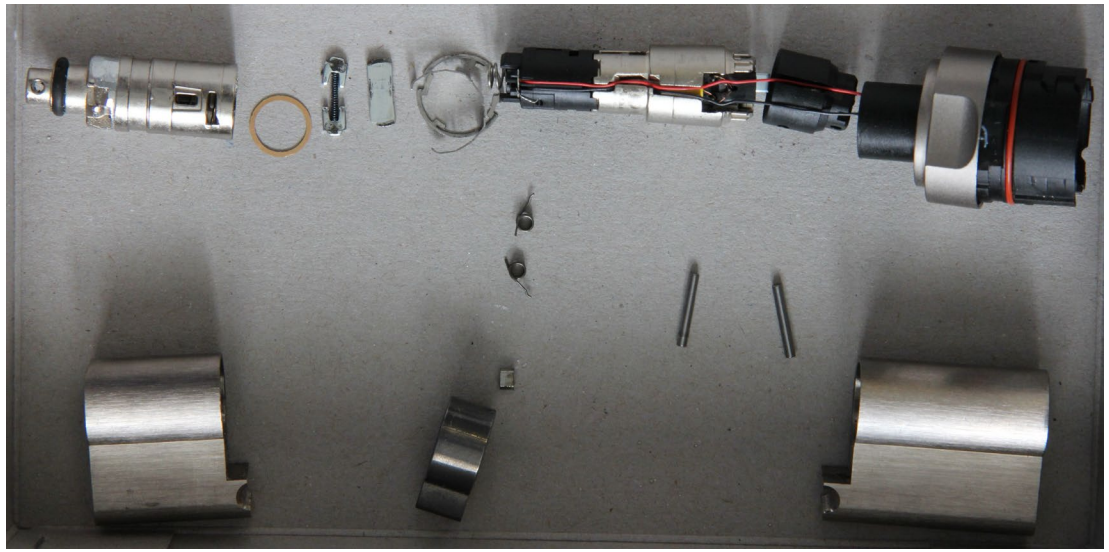
- Simons & Voss locks (2010-2013)
  - Published at ACM CCS 2013



Michael Weiner, Maurice Massar, Erik Tews, Dennis Giese and Wolfgang Wieser. 2013. Security analysis of a widely deployed locking system. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13). Association for Computing Machinery, New York, NY, USA, 929–940. https://doi.org/10.1145/2508859.2516733

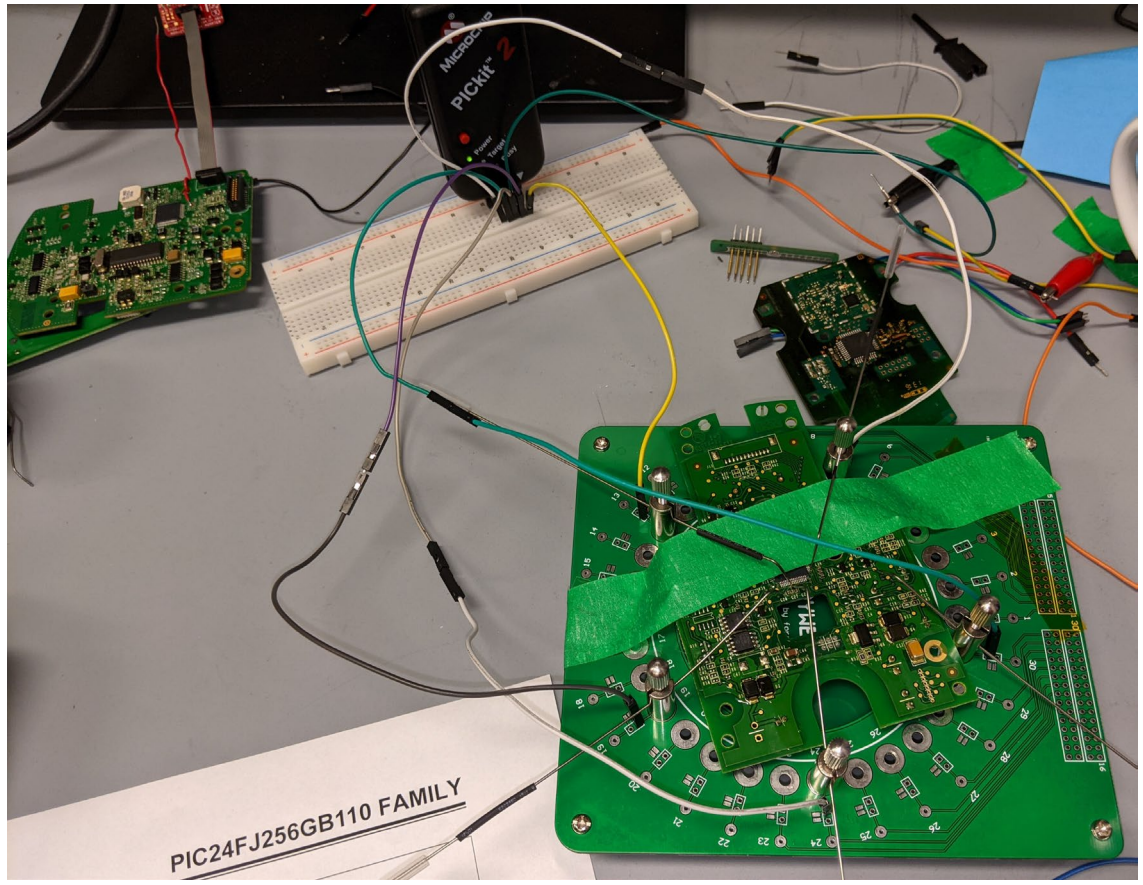






Previous work on locks

- Schlage AD-400/401 Electronic Locks (2017/2018)



Goals of this talk

- Overview of the reverse-engineering of “Digilock”, “SAG” locks
- Learn about vulnerabilities
- Understand methods to extract firmware and config
- Raise awareness about PIN numbers
- Sidenote:
  - We use Digilock and SAG as examples and are not claiming that they are more/less secure than other companies
  - We chose them due to their good reputations and quality of their products
  - We reported to the vendors. Digilock is actively working on fixing issues

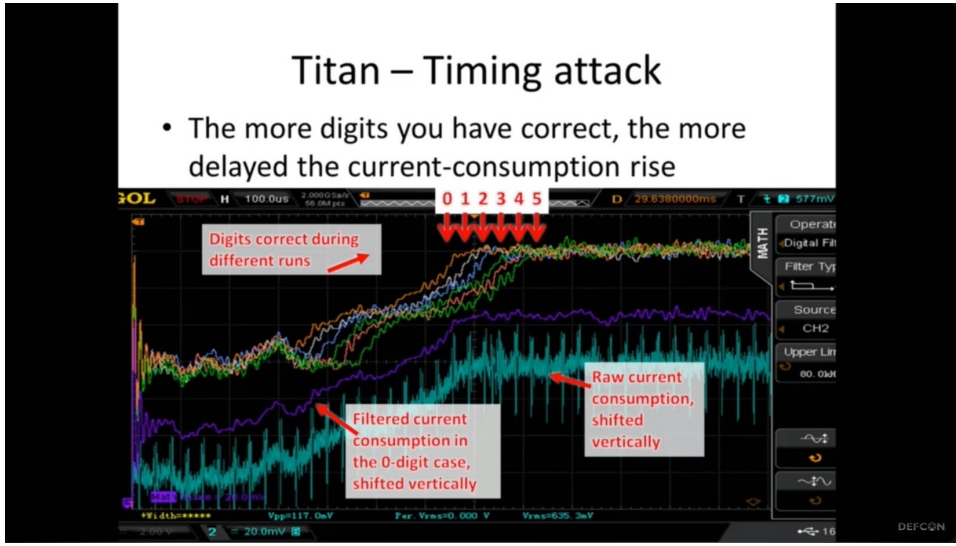
About this talk

- Continuation of our NULLcon Berlin 2024 talk
- Focus on offline, managed locks (e.g. master keyed)
- Does not cover
  - management software
  - re-provisioning
  - physical attacks using magnets
  - destructive attacks (drilling, decapping, etc.)
- We include a statement of Digilock in regard to their C&D

MOTIVATION

Motivation

- Hacking electronic locks is not new
- Researchers focus on high security safe locks
  - Lots of research in side-channel
  - Safes contain expensive things
  - Big impact if insecure



Problem: It is hard to defend against physical attacks and motivated attackers

https://www.reuters.com/article/us-locks-cyber-exclusive/exclusive-high-security-locks-for-government-and-banks-hacked-by-researcher-idUSKCN1UW26Z/
https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEF%20CON%2024%20-%20Plore-Side-Channel-Attacks-On-High-Security-Electronic-Safe-Locks.pdf
https://www.youtube.com/watch?v=lXFpCV646E0

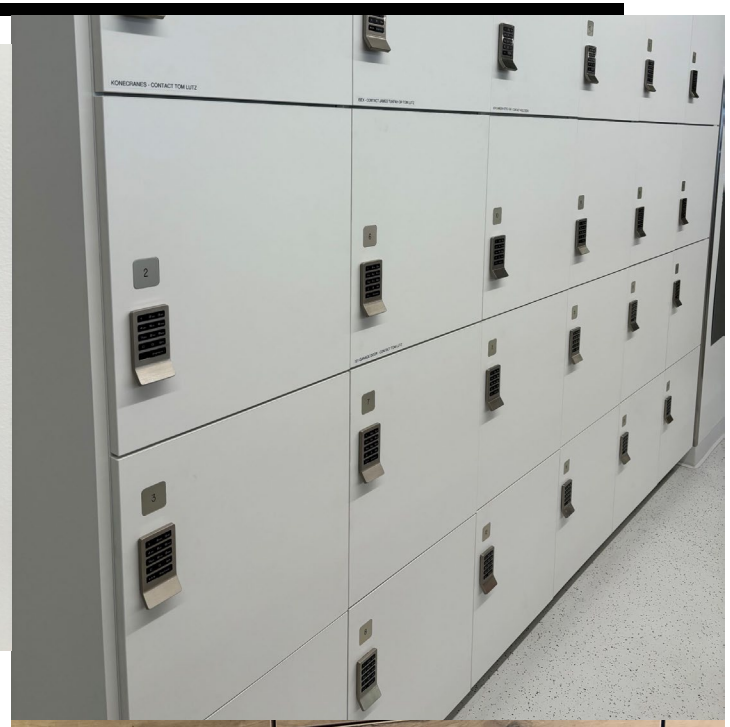
Motivation

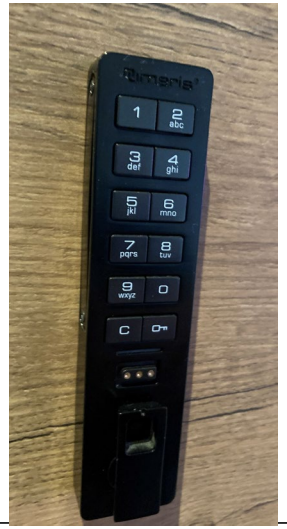
- Consumer locks, safes and cabinets are known to be bad
  - Mechanical flaws
  - Trivial bypasses
  - Insecure software

LockPickingLawyer: [1571] The DUMBEST “Safe” Design I’ve Ever Seen! (Toriexon)
https://www.youtube.com/watch?v=gJrSWXFXvlE

Motivation

- Northeastern University (~2018)
  - Lockers introduced to labs
  - locked with user-chosen PIN
- Also seen in
  - many co-working spaces
  - Banks
  - Airports
  - Hotels
  - Gyms





Top: Lockers in NEU EXP building
Bottom: Lockers in lobby of a Moxy Hotel in Germany

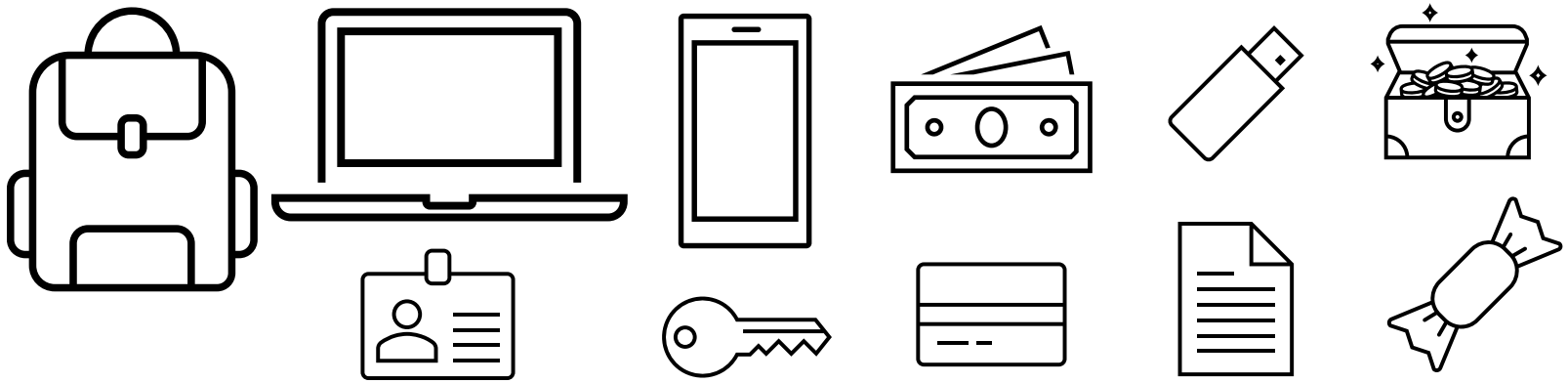
Motivation

- Only few, widely used vendors exist
- Locks stay in use for a very long time

Left: Digilock lockers in a gym in Seattle (thanks to @tihmstar)
Middle: SAG SAFE-O-TRONIC® lockers in a university in Germany
Right: Digilock lockers in a 5* hotel in Italy (thanks to @AapoOksman)

Why hack lockers/cabinets?

- Lockers and cabinets are everywhere
- Used in public spaces or shared workspaces
- Forgotten PIN, lost keys, Red Team penetration tests
- ~~Tamper with~~ correct audit logs
- Might contain interesting stuff (including our own)



Is the same PIN used for the locker as for the Phone, Notebook or Credit card?

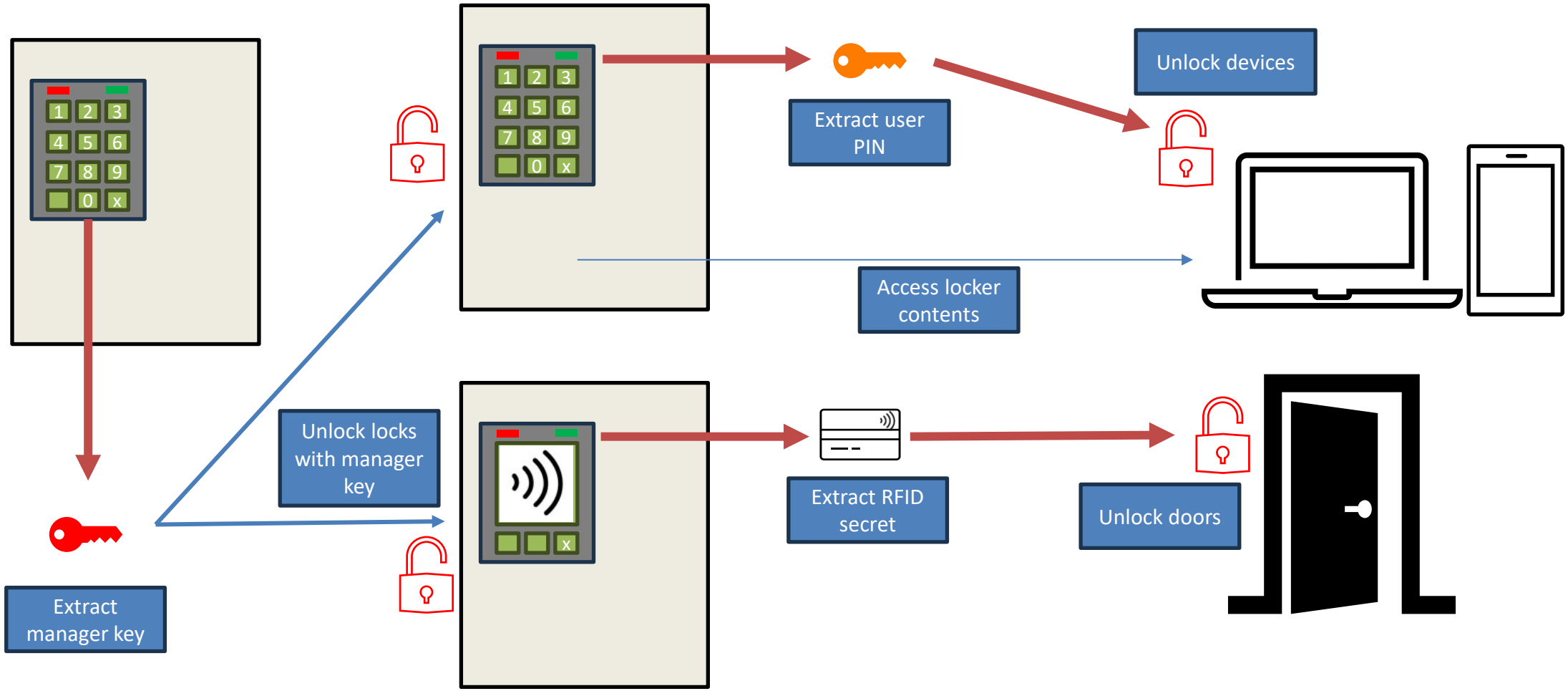
Quick survey:
Who knows “a friend” that is using a PIN in multiple places (e.g. Phone, Lockers, ATM cards)?

ATTACK IDEAS AND LOGISTICS

What are we looking for?

- Firmware
  - Find secret backdoors or bugs
  - Understand functionality
  - Create ~~malicious~~ custom firmware
- Interesting data
  - Key IDs, user PINs, RFID IDs, logs
- Ways to easily open locks

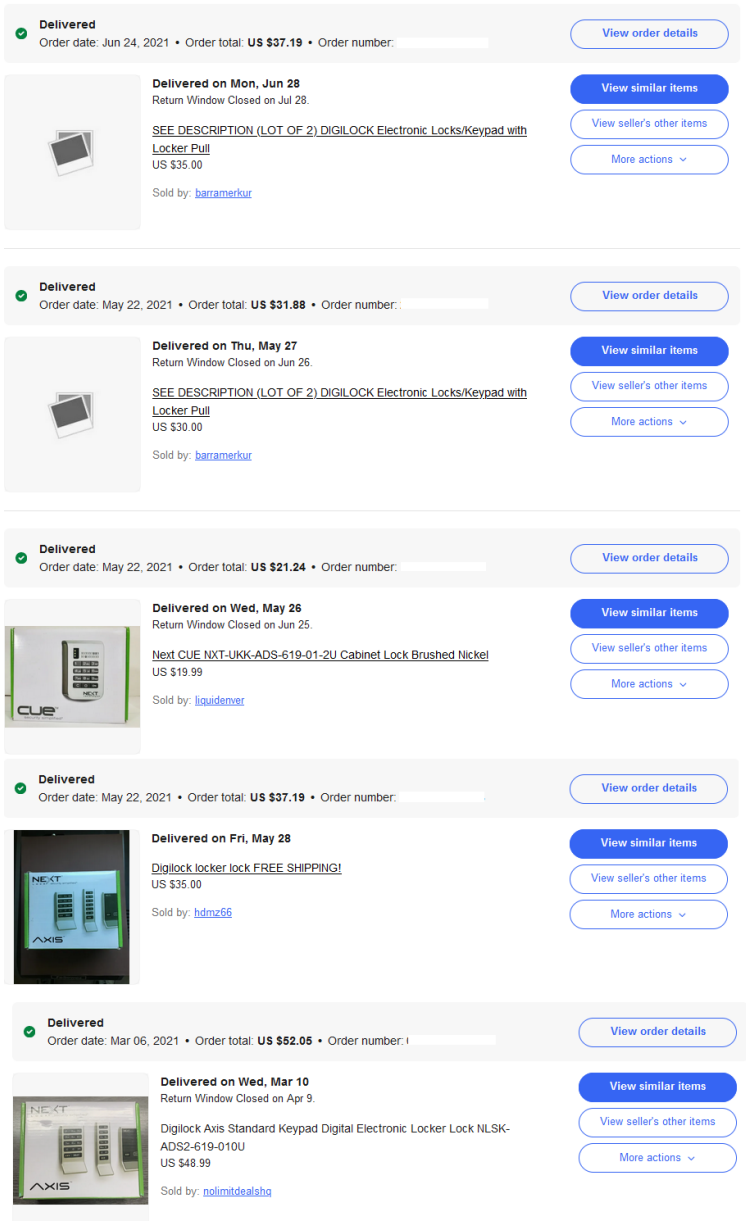
Idea: Lateral movement



Attack assumes that all lockers are in the same location
and provisioned with the same keys (e.g. programming keys, Master Keys, Manager keys etc.)
Typically, one master/manager key extracted from one installation wont work in another

Procurement

- Experiments require multiple devices
  - Cannot use someone else's property ☹
- Locks and Keys are expensive
  - Locks > USD $100, Keys > USD $50
- Surplus locks on eBay
  - Many gyms closed due to the pandemic
  - Cheap provisioned locks
  - New locks from failed projects



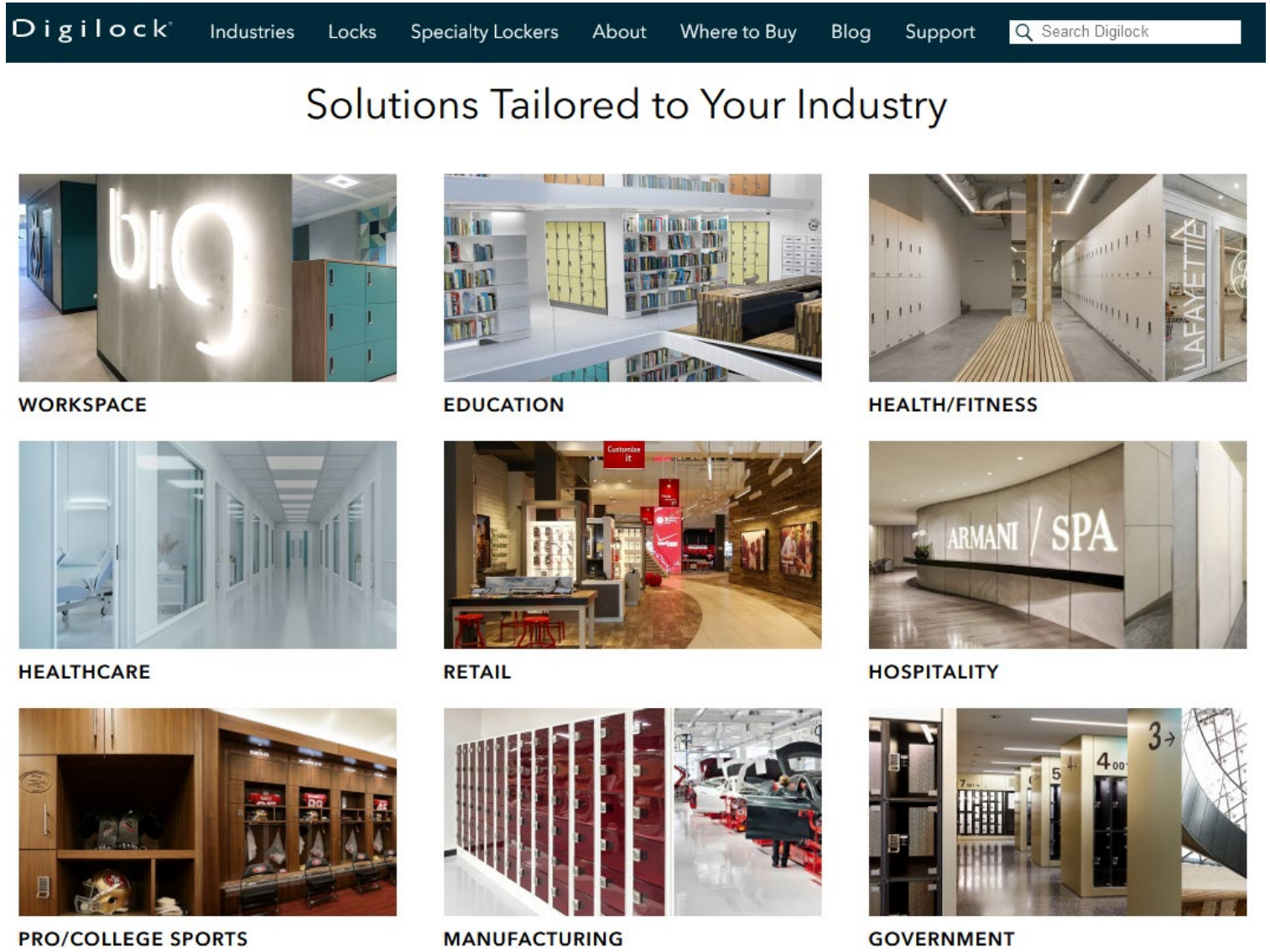
THE DIGILOCK ECOSYSTEM

Digilock

- Brand of Security People Inc. (US based)
- Over 40 years in the industry
- “global leader in keyless lock solutions”
- Many different types and brands of locks
  - Connected locks, offline locks, mechanical locks
  - Access medium: RFID, PIN, key fobs, smartphone (BLE)
  - Brands (examples): “Digilock”, “NEXT”, “Numeris”

Source(March 2024): https://digilockeurope.com/en/

Industries



Source/Screenshot(March 2024): https://www.digilock.com/

Examples

Lock Hardware

- All locks have similar hardware
  - Similar type of MCU
- No tamper switches
- Locking state controlled by latch
- Protection against physical attacks
- Features depend on brand
  - Audit support
  - Assigned/shared locker functionality

Different brands of Digilock locks (AXIS, CUE, AXIS, 4G)

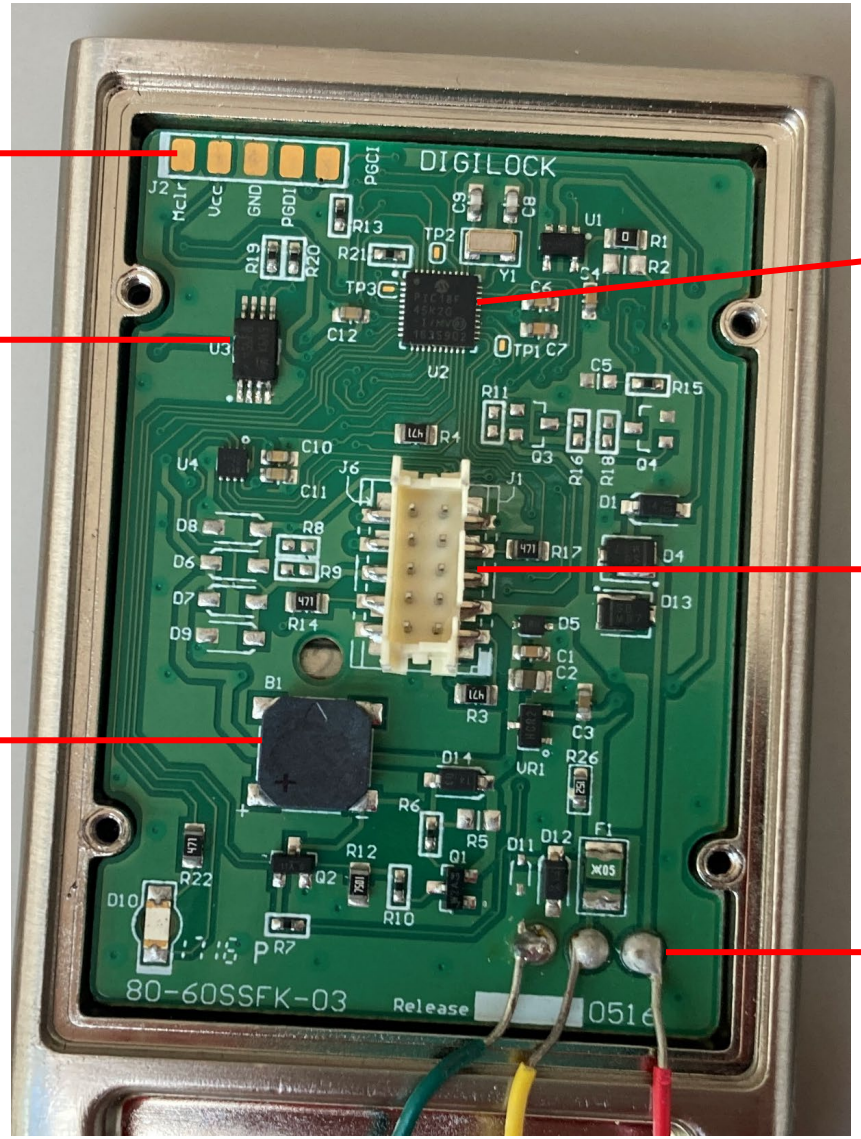
Lock Hardware

PWR 1W GND

PIC programming interface

EEPROM

Piezo



MCU

Connection to inside latch (BAT, lock state, motor control)

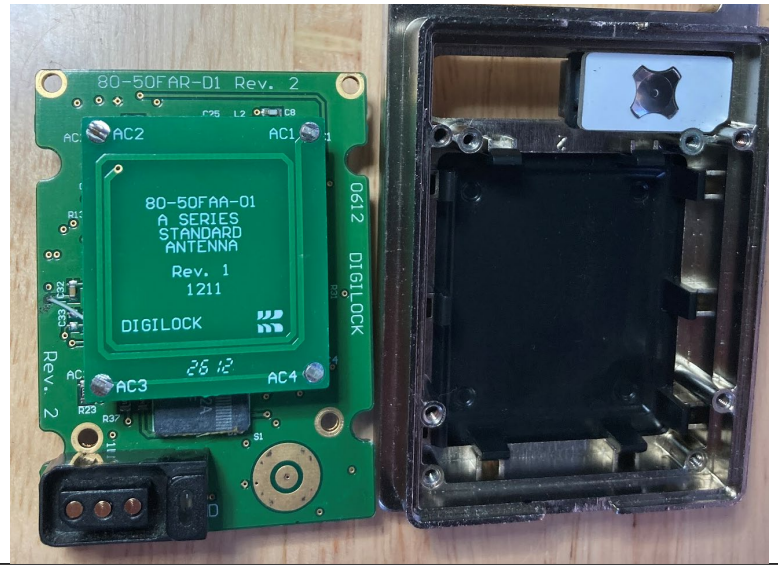
Interface (GND,1W,PWR)

Digilock NEXT AXIS lock backside of PCB

Lock Hardware

- Micro Controller (MCU)
  - PIC18F45K20/PIC18F25K20
  - PIC24FJ256GA
- EEPROM (for audit or credentials storage)
  - serial I²C bus EEPROM
- RFID
  - ST ST25R3911B
  - LEGIC SM-6300 (+HSM+BLE)

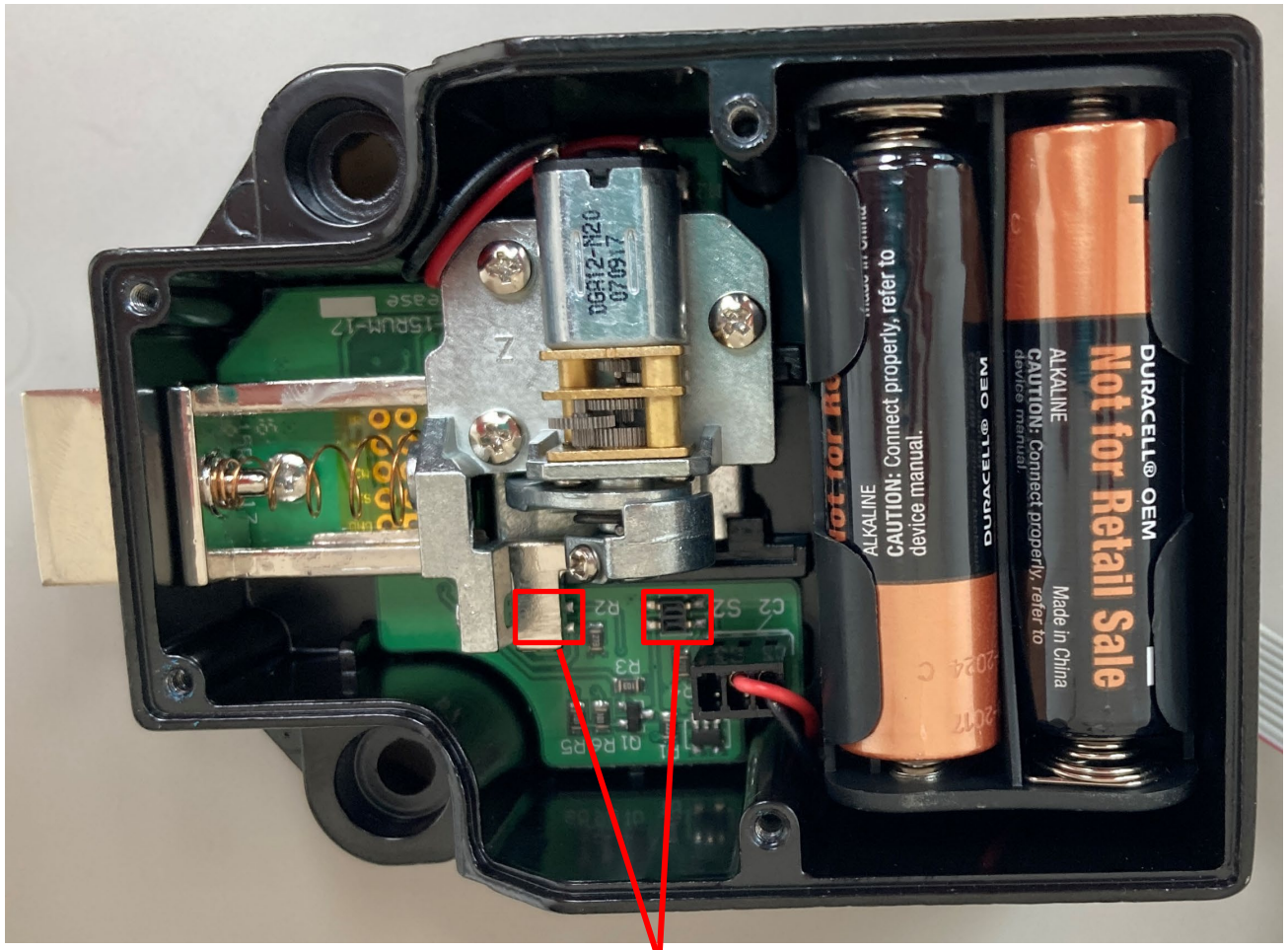
Supposedly the HSM is used on new locks



Digilock 4G RFID PCB front and backsides

Lock Hardware

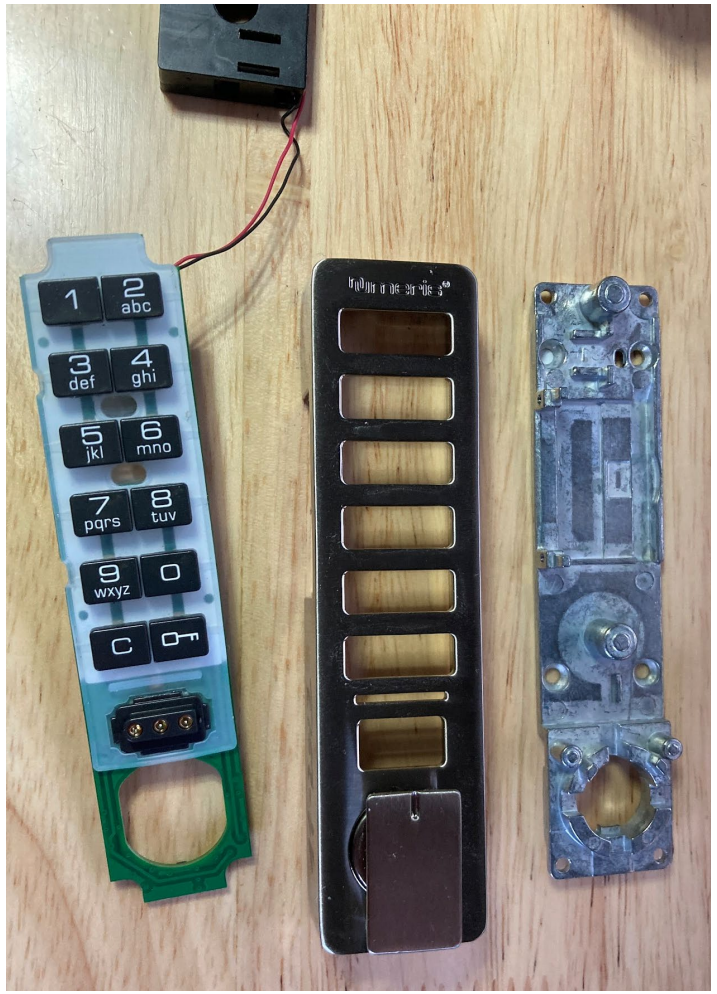
Digilock 4G (outside part) with latch unit (inside part)



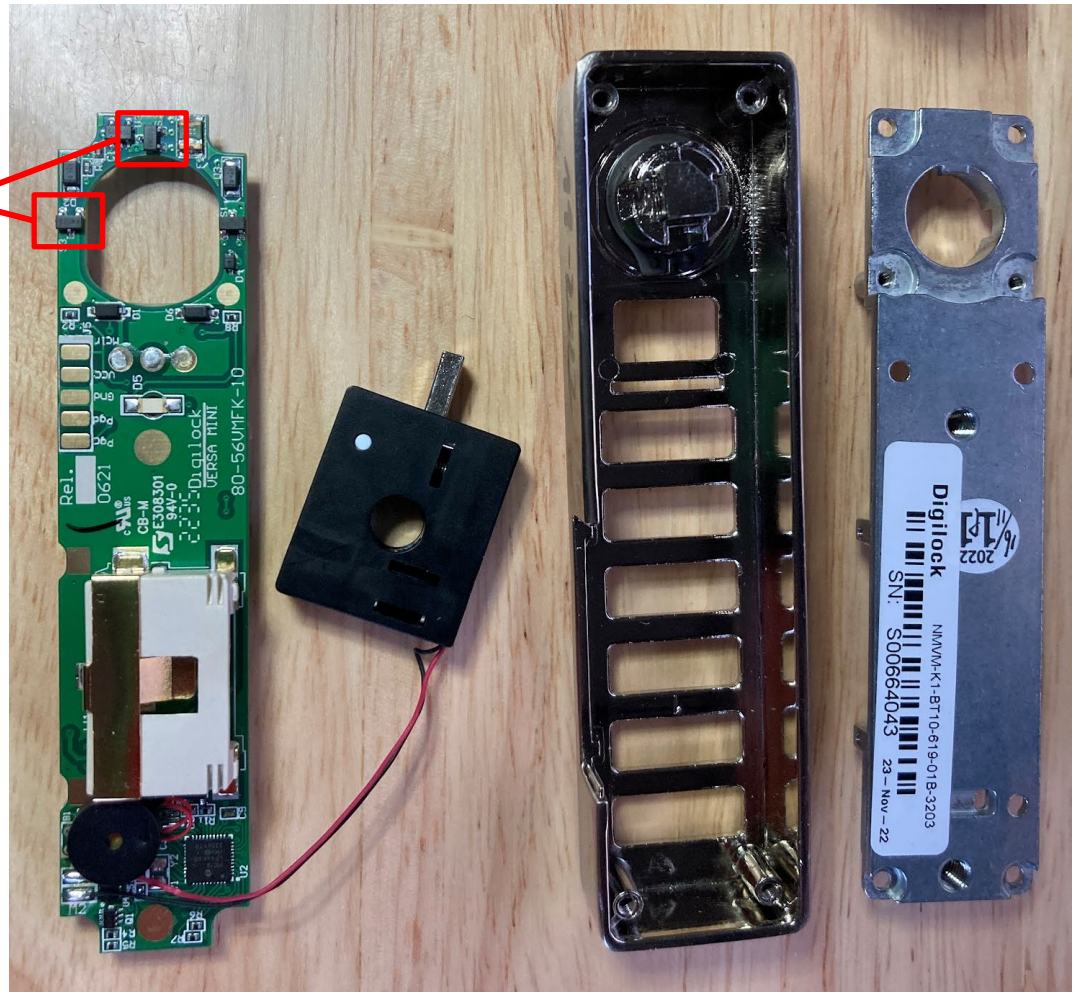
Reed contacts
for lock state

Opened latch unit

Lock Hardware



Reed contacts
for lock state



Digilock Versa Mini teardown

Keys

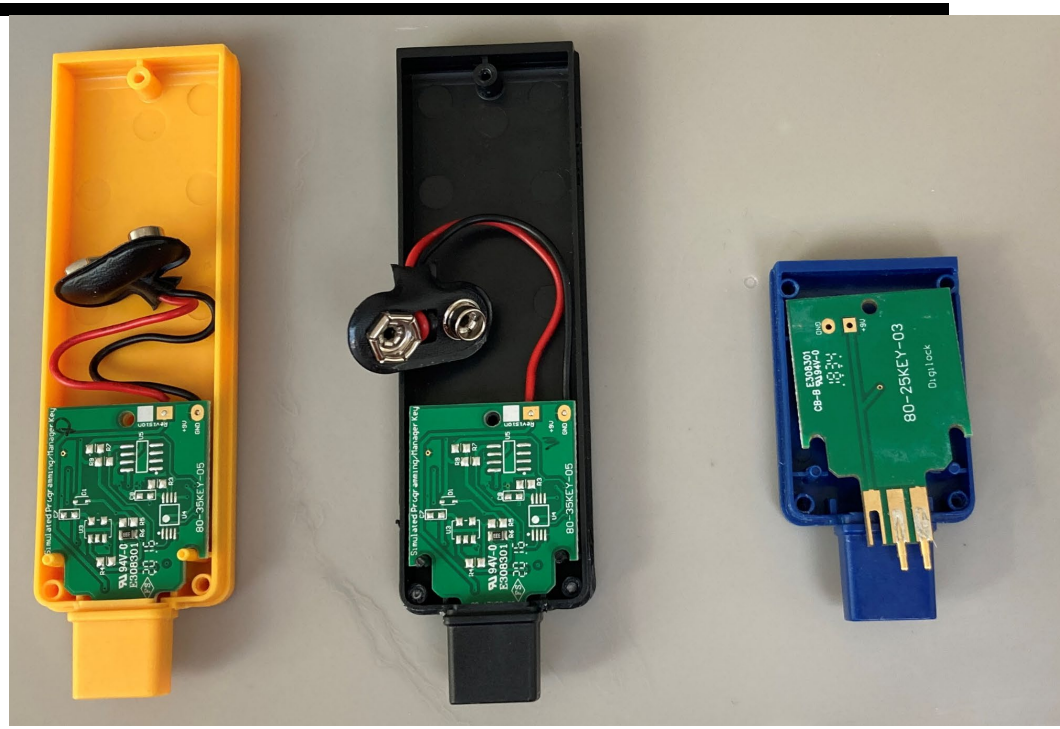
- Programming Key (yellow)
  - Only one exists per “locking system”
  - Adds/removes manager keys
  - Allows lock override
  - Power for a dead lock
  - Cloning configuration/audits/etc.
- Manager Keys (black)
  - Allows lock override
  - Power for a dead lock
- ADA Key (blue)
  - Alternative to PIN / RFID

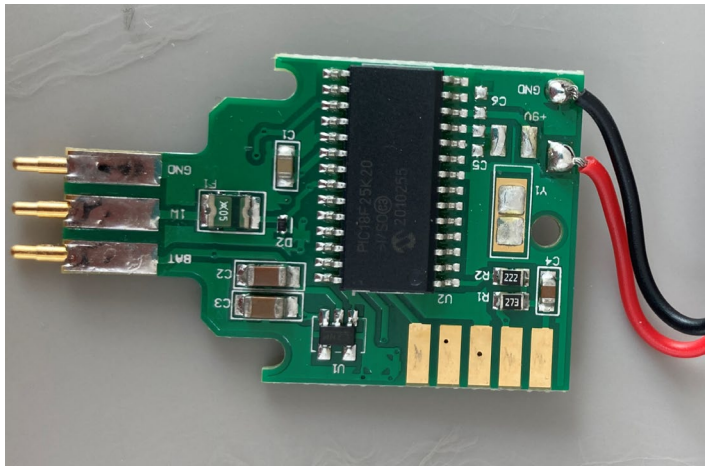
Digilock keys: Programming, Manager, ADA, Reset

ADA: “Americans with Disabilities Act”

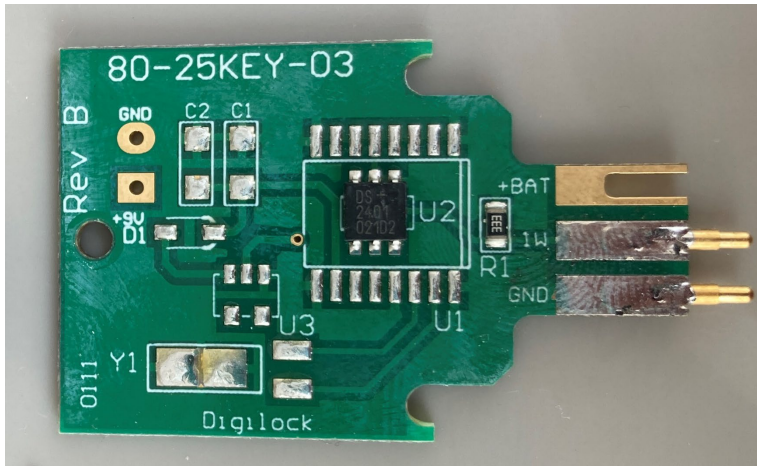
Keys

- Programming/Manager key
  - Same hardware, different case color
  - 9V battery
  - PIC18F25K20
  - PIC programming interface
- ADA key
  - DS2401 aka iButton
  - 48 bit ID





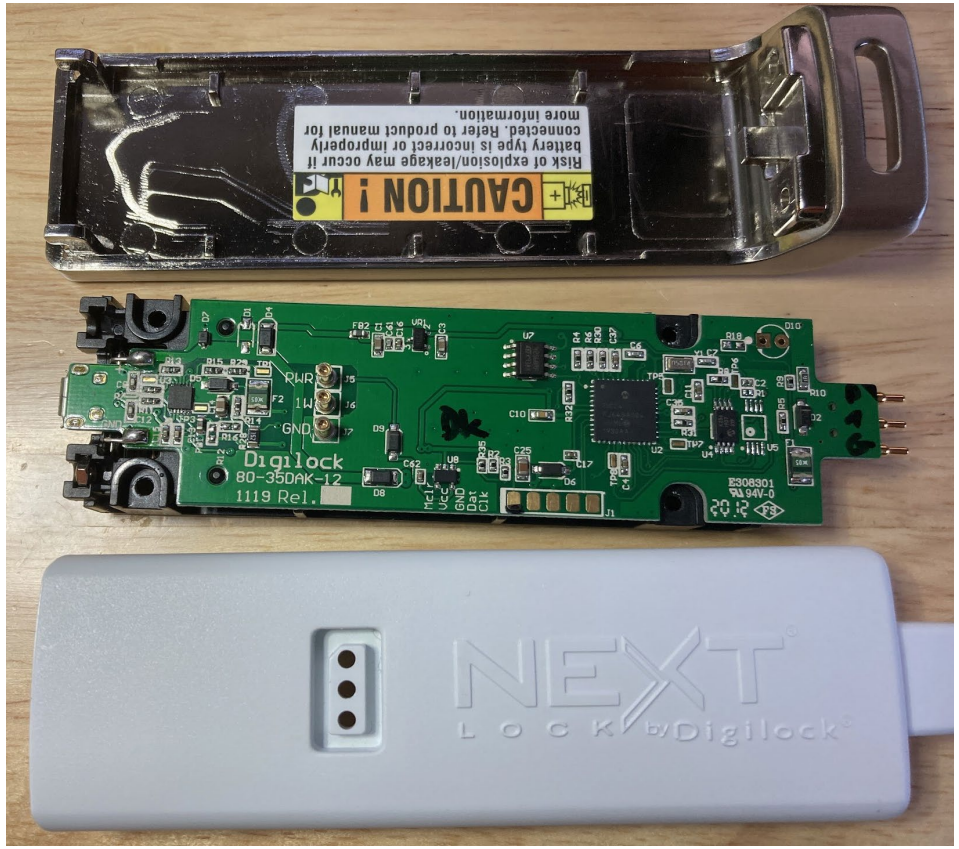
Programming key



ADA key

Keys

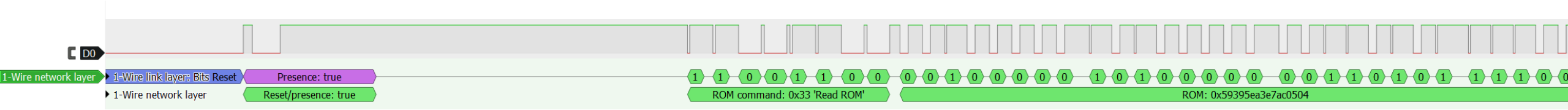
- Data Key
  - Connects to tablet via USB
  - Works like a programming/manager key
  - Advanced functionality (Audits, etc.)
  - PIC24FJ64
  - PIC programming interface



One Wire communication

- Interception with logic analyzer
- Usage of “Read ROM” command
- Keys return 8 bytes of ID (7 Data + 1 CRC8)
- Key types identified by first byte of ID
- Bus resets after transaction

No cryptographic operations used



Trace of programming key authentication

PIC MCUS

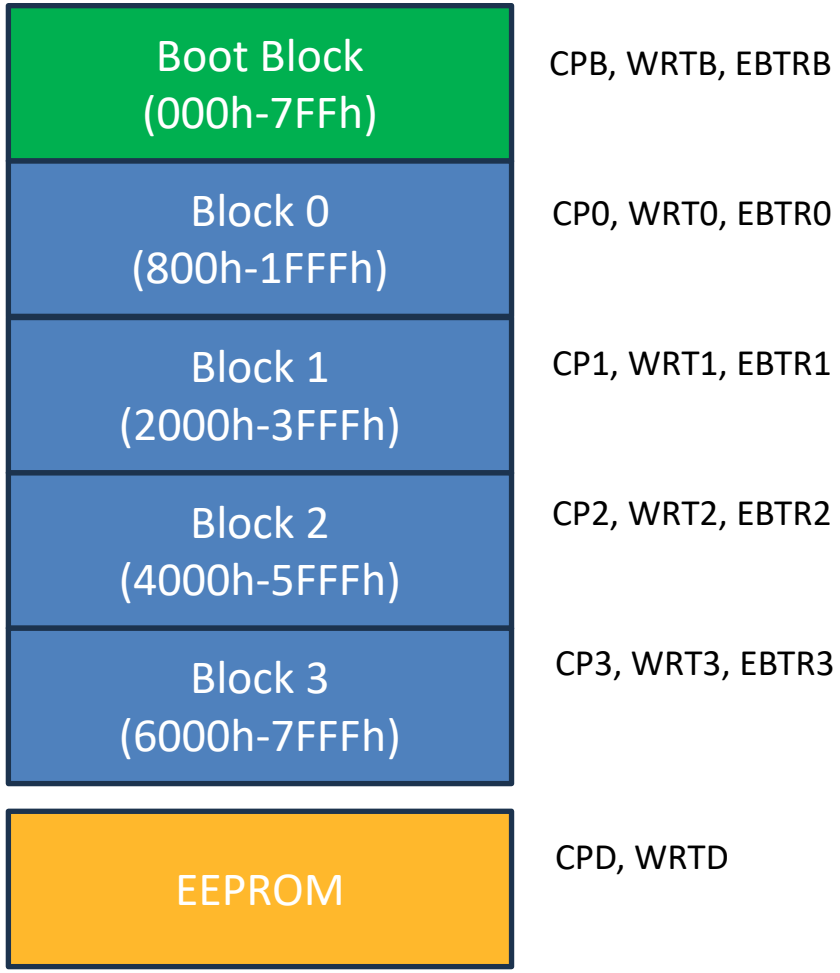
PIC intro

- MCU by Microchip
- Very common for locks
  - Used by Simons&Voss, Schlage, Kitlock, Aqara, etc.
  - Low power, ideal for battery operation
- PIC18
  - 8 Bit MCU, released 2000
- PIC24
  - 16 bit MCU
  - No on-chip Data EEPROM

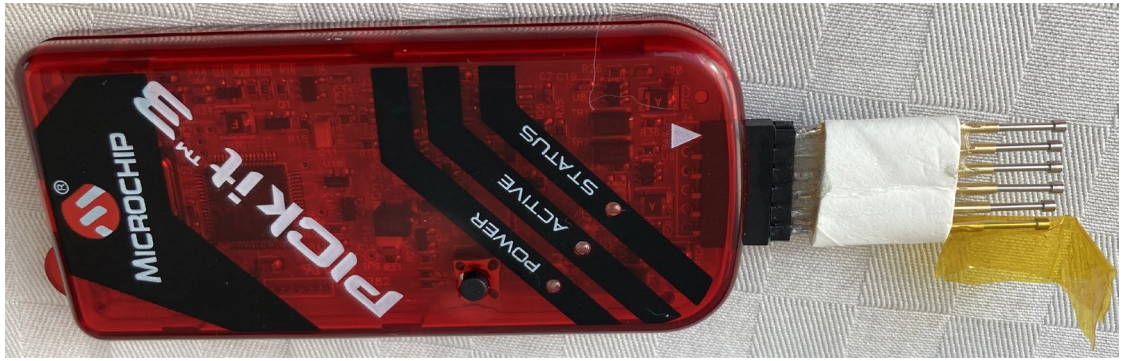
https://www.microchip.com/en-us/products/microcontrollers-and-microprocessors

Example: PIC18F25K20

- 1536 Bytes SRAM
- 32 KBytes Flash
- 256Bytes EEPROM
- Protections
  - Code Protection (CP)
  - Write Protection (WRT)
  - External Block Table Read (EBTRB)



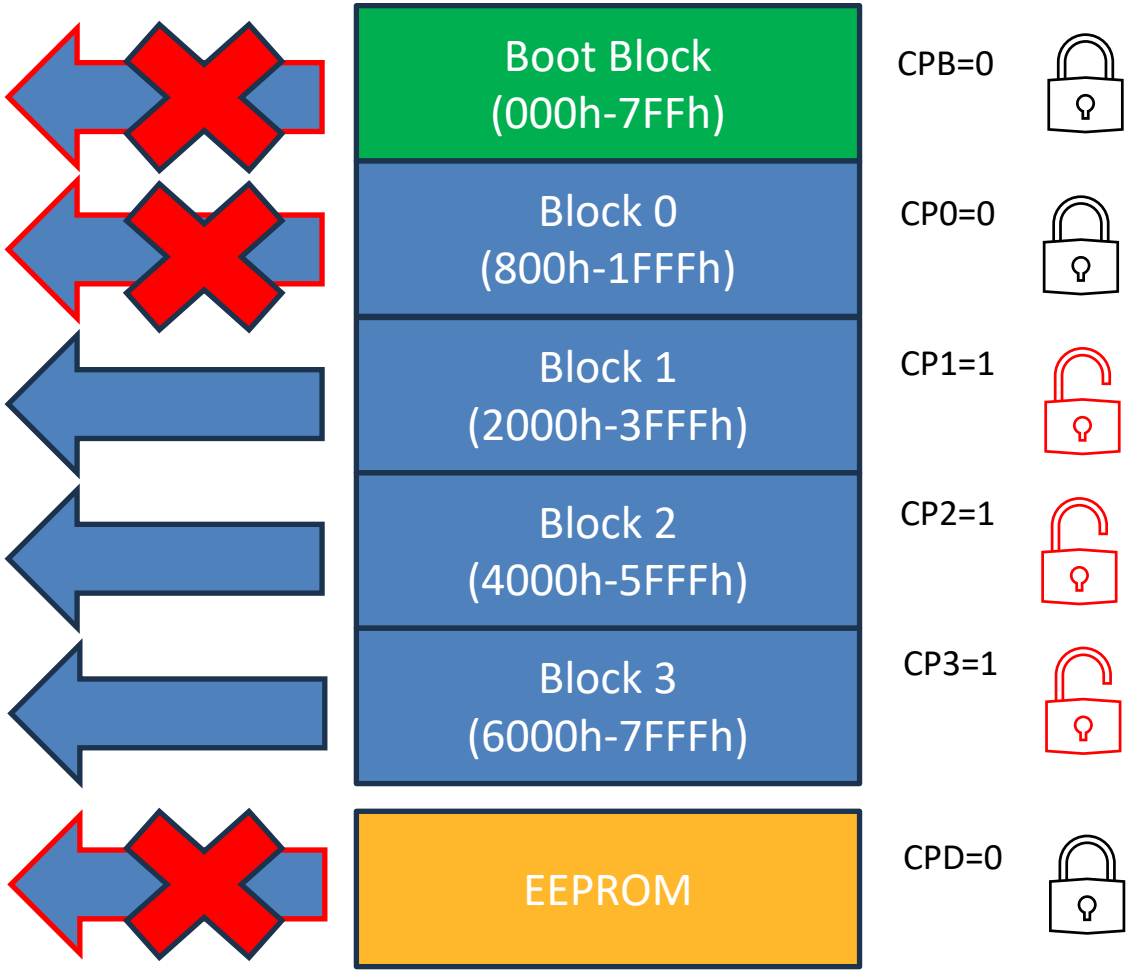
Code Protection example



Microchip Pickit debugger

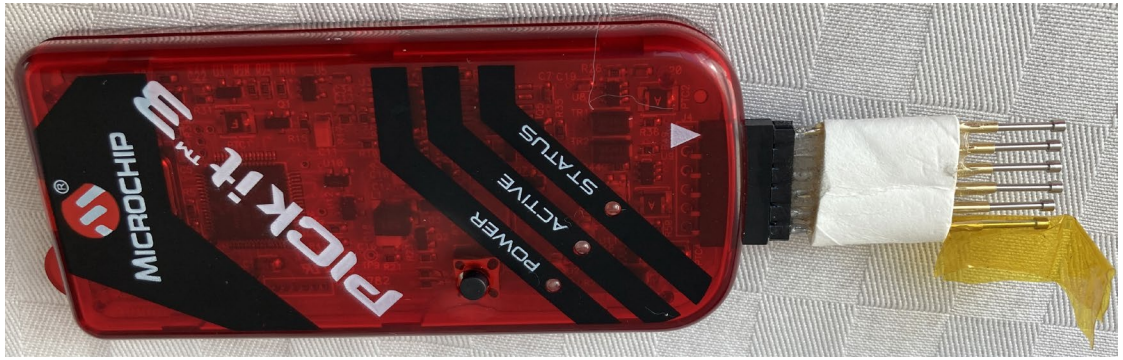
- Blocks Boot, 0 and Data return 0's
- Blocks 1,2,3 return data

Code Protection (CP) is also known as Readout Protection (RDP)



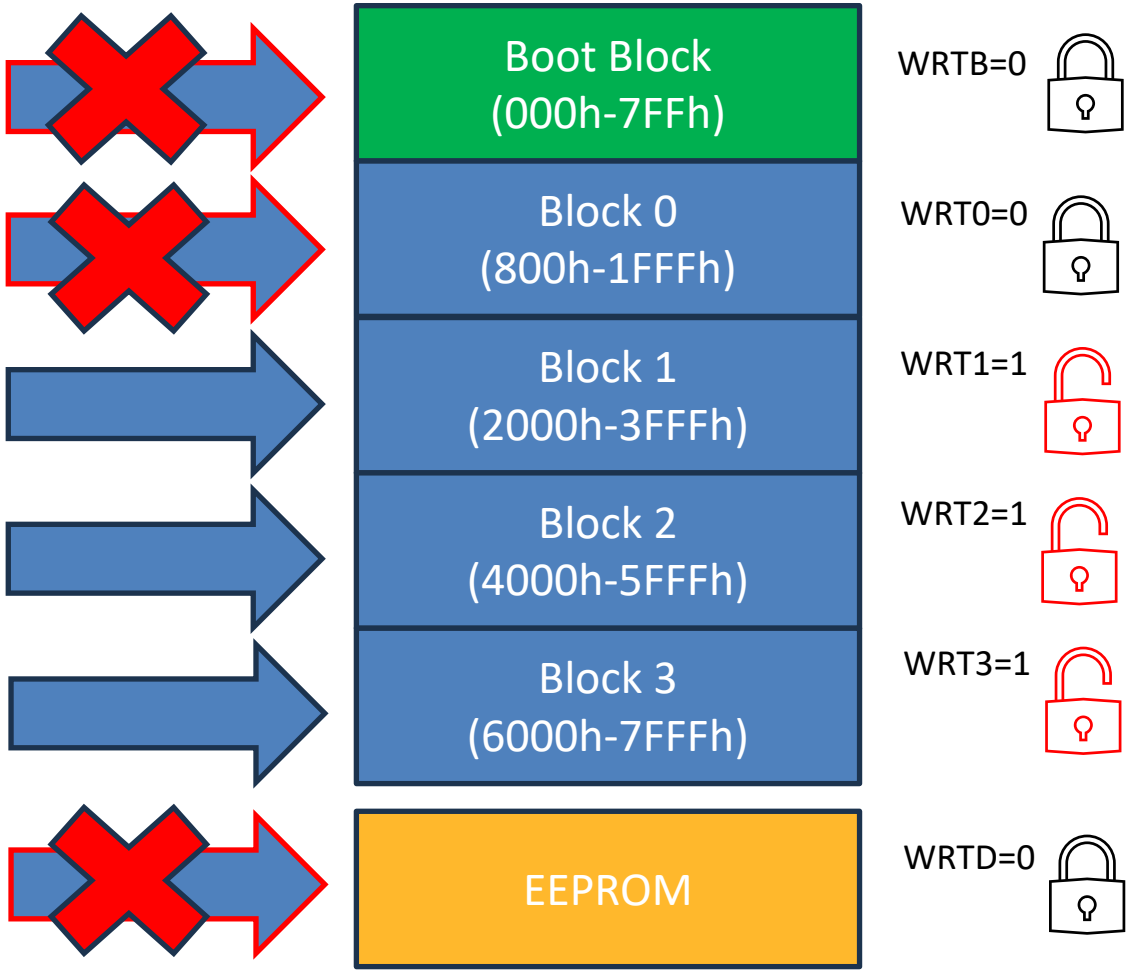
Fictitious example of a programmed PIC MCU
bit 1=default off, bit 0=enabled

Write Protection example



Microchip Pickit debugger

- Blocks Boot, 0 and Data fail writes
- Blocks 1,2,3 are programmed



Fictitious example of a programmed PIC MCU
bit 1=default off, bit 0=enabled

PIC Security

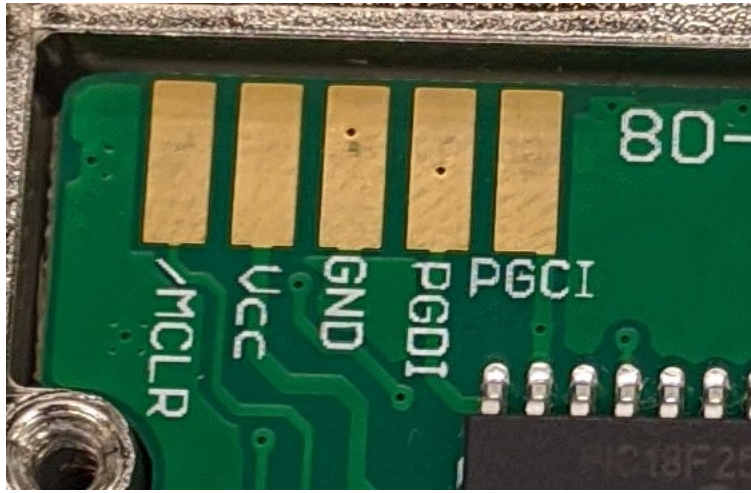
- MCUs offer only basic protection against attacks
- Many attacks exist (even if protections are enabled)
  - Optical/Laser attacks in 2002
  - UV erasure of config bits
  - Glitching
  - Overwriting individual blocks to dump other blocks

Examples:
Skorobogatov, Sergei & Anderson, Ross. (2002). Optical Fault Induction Attacks. Optical Fault Induction Attacks. 2523. 2-12. 10.1007/3-540-36400-5_2.
https://www.bunniestudios.com/blog/?page_id=40
http://blog.lanka.sk/2013/11/hacking-apc-back-ups-hs-500.html

ATTACKS

Dumping flash and EEPROM

- Naive approach: connect debugger and dump MCU flash
  - Debug pins were exposed on all locks and keys
  - Finding: very inconsistent protection settings



Dumping flash and EEPROM

- General observation:
  - No write protection
  - External EEPROMs not encrypted

	Code protected?	EEPROM protected?
manager, programming keys (PIC18 based)	yes *	no
Data key (PIC24 based)	no	no
PIN locks (PIC18F based, older gens)	yes *	no
RFID locks (PIC24F based)	no	no
PIN locks (PIC18LF based, new gens)	no	no

Locks/Keys manufactured between August 2014 and November 2022

```
:020000040000FA
:100000000000000000000000000000000000000000F0
:100010000000000000000000000000000000000000E0
:100020000000000000000000000000000000000000D0
:100030000000000000000000000000000000000000C0
:100040000000000000000000000000000000000000B0
:100050000000000000000000000000000000000000A0
:100060000000000000000000000000000000000000 90
:100070000000000000000000000000000000000000 80
:100080000000000000000000000000000000000000 70
:100090000000000000000000000000000000000000 60
:1000A0000000000000000000000000000000000000 50
:1000B0000000000000000000000000000000000000 40
:1000C0000000000000000000000000000000000000 30
:1000D0000000000000000000000000000000000000 20
:1000E0000000000000000000000000000000000000 10
:1000F0000000000000000000000000000000000000 00
:100100000000000000000000000000000000000000EF
:100110000000000000000000000000000000000000DF
:100120000000000000000000000000000000000000CF
:100130000000000000000000000000000000000000BF
:100140000000000000000000000000000000000000AF
:100150000000000000000000000000000000000000 9F
:100160000000000000000000000000000000000000 8F
:100170000000000000000000000000000000000000 7F
:100180000000000000000000000000000000000000 6F
:100190000000000000000000000000000000000000 5F
:1001A0000000000000000000000000000000000000 4F
:1001B0000000000000000000000000000000000000 3F
:1001C0000000000000000000000000000000000000 2F
:1001D0000000000000000000000000000000000000 1F
:1001E0000000000000000000000000000000000000 0F
:1001F0000000000000000000000000000000000000 FF
:100200000000000000000000000000000000000000EE
:100210000000000000000000000000000000000000DE
:100220000000000000000000000000000000000000CE
:100230000000000000000000000000000000000000BE
:100240000000000000000000000000000000000000AE
:100250000000000000000000000000000000000000 9E
:100260000000000000000000000000000000000000 8E
```

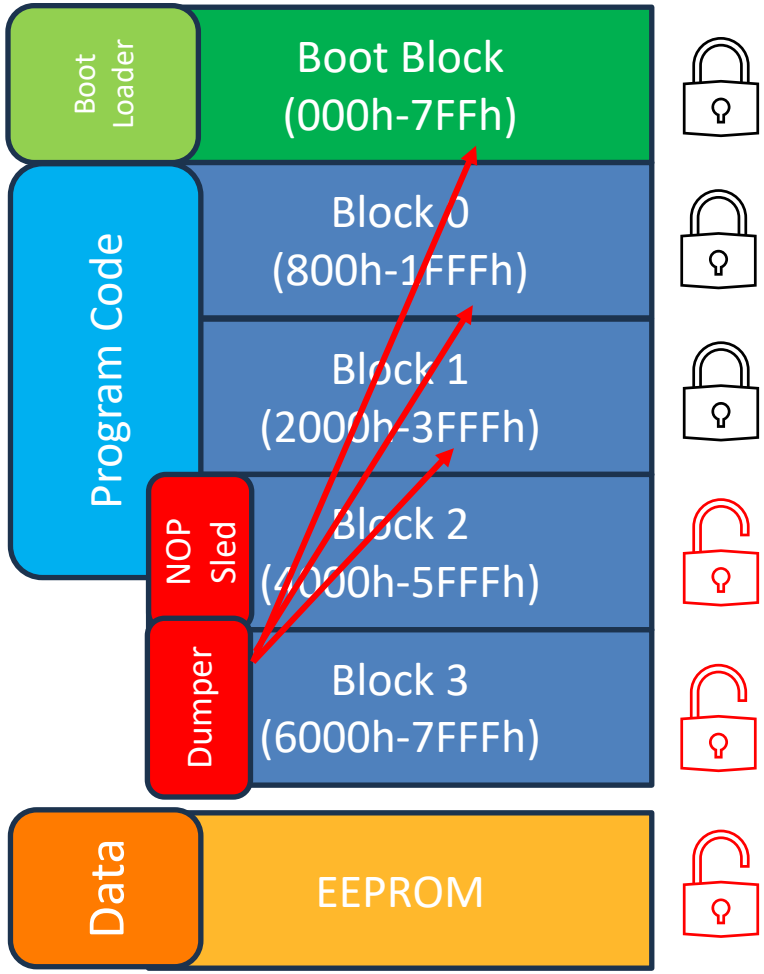
Output of flash read for protected lock

* Partially protected, only “boot block” and block 0-1

For a full overview check: https://dontvacuum.me/talks/DEFCON32-locks

Dumping flash and EEPROM

- For unprotected devices
  - Dump Code Memory and EEPROM directly
- For partially protected devices
  - Use of custom dumper to exfiltrate firmware
  - Access EEPROM memory directly
- Attacks described in our NULLCON Berlin 2024 talk



Code/Data on NEXT CUE lock

https://dontvacuum.me/talks/NULLconBerlin2024/ (page 36-40)

Dumping flash and EEPROM

- Firmware extraction successful for all locks
- Binary can be analyzed and modified
  - Ghidra has PIC support
  - No signatures or integrity checks
- Method well known and established

```
Address    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F  ASCII

000007B0:  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007C0:  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007D0:  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007E0:  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007F0:  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
00000800:  01 01 EA 6A E3 25 E9 6E  E4 51 EA 22 EF 50 0B 08  ...j.%.n.Q.".P..
00000810:  05 E1 E9 EC 10 F0 00 0E  27 D1 54 D0 01 01 D9 50  ........'.T....P
00000820:  03 0F E3 6F DA CF E4 F1  01 50 01 01 EA 6A E3 25  ...o.....P...j.%
00000830:  E9 6E E4 51 EA 22 EF 50  66 08 27 E1 00 01 99 05  .n.Q.".Pf.'.....
00000840:  1F E1 00 01 07 0E 69 6F  02 6A 02 50 03 08 13 E3  ......io.j.P....
00000850:  02 50 EA 6A 99 0F E9 6E  00 0E EA 22 EF CF E6 FF  .P.j...n...".....
00000860:  69 C0 E6 FF 8E EC 16 F0  42 E9 00 01 69 29 00 01  i.......B...i)..
00000870:  69 6F 02 2A EA D7 85 EC  11 F0 01 0E F5 D0 04 D0  io.*............
00000880:  E9 EC 10 F0 01 0E F0 D0  1D D0 03 50 09 08 0E E3  ............P...
00000890:  04 50 09 08 0B E3 05 50  09 08 08 E3 06 50 09 08  .P.....P.....P..
000008A0:  05 E3 0B 0E 07 5C 02 E1  10 D0 0C D0 0B 0E 03 5C  .....\.........\
000008B0:  08 E1 0B 0E 04 5C 05 E1  E9 EC 10 F0 00 0E D4 D0  .....\..........
000008C0:  01 D0 00 00 01 28 01 6E  44 D7 85 EC 11 F0 01 0E  .....(.nD.......
000008D0:  E6 6E 15 EC 13 F0 41 E9  01 6A 3F DE E6 6E 01 01  .n....A..j?..n..
000008E0:  D9 50 08 0F E3 6F DA CF  E4 F1 01 50 01 01 EA 6A  .P...o.....P...j
000008F0:  E3 25 E9 6E E4 51 EA 22  E5 52 E7 50 EF 6E D5 9E  .%.n.Q.".R.P.n..
00000900:  01 0E E6 6E 15 EC 13 F0  41 E9 F2 A4 02 D0 00 0E  ...n....A.......
00000910:  AB D0 01 01 D9 50 08 0F  E3 6F DA CF E4 F1 01 50  .....P...o.....P
00000920:  01 01 EA 6A E3 25 E9 6E  E4 51 EA 22 EF 50 0C 08  ...j.%.n.Q.".P..
00000930:  16 E1 02 6A 02 50 04 08  10 E3 01 01 D9 50 08 0F  ...j.P.......P..
00000940:  E3 6F DA CF E4 F1 01 50  01 01 EA 6A E3 25 E9 6E  .o.....P...j.%.n
00000950:  E4 51 EA 22 EF 68 02 2A  ED D7 01 68 80 D0 04 0E  .Q.".h.*...h....
00000960:  01 5C 15 E2 01 01 D9 50  08 0F E3 6F DA CF E4 F1  .\.....P...o....
00000970:  01 50 01 01 EA 6A E3 25  E9 6E E4 51 EA 22 EF 50  .P...j.%.n.Q.".P
00000980:  0B 08 05 E1 E9 EC 10 F0  00 0E 6E D0 68 D0 04 0E  ..........n.h...
00000990:  01 5C 59 E1 0B 0E 0C 5C  04 E0 E9 EC 10 F0 00 0E  .\Y....\........
000009A0:  63 D0 02 6A 02 50 03 08  26 E3 01 01 D9 50 08 0F  c..j.P..&....P..
000009B0:  E4 6F DA CF E5 F1 02 50  01 01 EA 6A E4 25 E9 6E  .o.....P...j.%.n
000009C0:  E5 51 EA 22 EF CF E3 F1  01 01 D9 50 03 0F E6 6F  .Q.".......P...o
000009D0:  DA CF E7 F1 02 50 01 01  EA 6A E6 25 E9 6E E7 51  .....P...j.%.n.Q
000009E0:  EA 22 EF 50 01 01 E3 5D  04 E0 E9 EC 10 F0 00 0E  ."P...].........
000009F0:  3B D0 02 2A D7 D7 03 EB  E6 FF 07 0E E6 6E 8E EC  ;..*.........n..
00000A00:  16 F0 42 E9 04 EB E6 FF  08 0E E6 6E 8E EC 16 F0  ..B........n....
00000A10:  42 E9 05 EB E6 FF 09 0E  E6 6E 8E EC 16 F0 42 E9  B........n....B.
00000A20:  06 EB E6 FF 0A 0E E6 6E  8E EC 16 F0 42 E9 85 EC  .......n....B...
00000A30:  11 F0 0A 0E E6 6E BA EC  16 F0 41 E9 85 EC 11 F0  .....n....A.....
00000A40:  01 0E 12 D0 0C D0 0B 0E  08 5C 08 E1 0B 0E 09 5C  .........\.....\
00000A50:  05 E1 E9 EC 10 F0 00 0E  07 D0 01 D0 00 00 01 28  ................(

                                                            0x00000000 - 0x00007FF
```

EEPROM contents

- Requires trial and error to find data fields and meaning
- Differs between lock generations

Observation: Some locks do not wipe the PIN/User key after unlocking. Some versions do.

partial Programming Key ID

# of Manager Keys

Failed PIN counter

PIN, ADA Key ID or RFID UID*

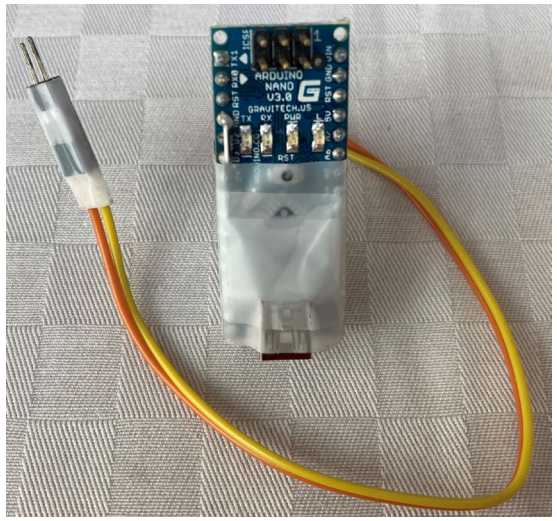
Address	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	ASCII
00	41	05	05	AC	E7	01	00	01	02	03	04	00	00	FF	59	11	A..... .....Y.
10	FF	FF	FF	78	57	67	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	...xWg.. .....
20	14	63	F5	D7	0E	8F	D7	71	FF	FF	FF	FF	FF	FF	FF	FF	.c.....q .....
30	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	

Hexdump of fully provisioned Gen4 lock, one manager key, PIN 1234 set

Manager Key ID

*only the UID is saved (MIFARE, ISO14443A), no cryptographic keys

Emulation/Cloning Keys



- Applies to both RFIDs and Keys
- Only ID is required for cloning
  - Extraction from key or flash
- Can be emulated:
  - Arduino
  - Flipper Zero
  - Proxmark (RFIDs only)

Other attacks possibilities

- Bruteforce PINs and keys *
- Sidechannel attacks *
- Cloning lock configuration via OneWire
- Modifying contents of audit EEPROM
- Usage of malicious firmware

*Attacks described in our NULLCON Berlin 2024 talk
https://dontvacuum.me/talks/NULLconBerlin2024/

“Cease&Desist” incident

- Received C&D email at 2:16pm on 08.08.2024 (day before talk)
  - Copyright Act, Defend Trade Secret Acts, State trade secret law, Computer Fraud and Abuse Act, Digital Millenium Copyright Act
- By 3:30pm meeting with Hannah Zhao (EFF) and Kurt Opsahl
- Moved talk from Friday to Sunday
- Phone call with everyone involved on Saturday evening
  - Exchanged views and amicably resolved differences
- C&D withdrawn in writing at 0:24am on 11.08.2024

Summarized Digilock response

- Acknowledged communication about improvements prior to DEFCON
- Improvements:
  - Code protection to all data blocks
  - Implementation of code protection to PIC18 and PIC24
  - Communication encryption to prevent cloning via UID
  - EEPROM data encryption (at rest and in transit)
- In over 32 years no reported security incident due to a hacked lock
- Digilock is fully committed to providing secure solutions for its customers.
- Full statement on slide 71.

SCHULTE-SCHLAGBAUM AG (SAG)

Schulte-Schlagbaum AG (SAG)

- German company, existing since 1833
- Widely used in Europe/Germany
  - mechanic and electronic locker locks
  - Brand: SAFE-O-TRONIC ®
  - Door* and cabinet/locker products

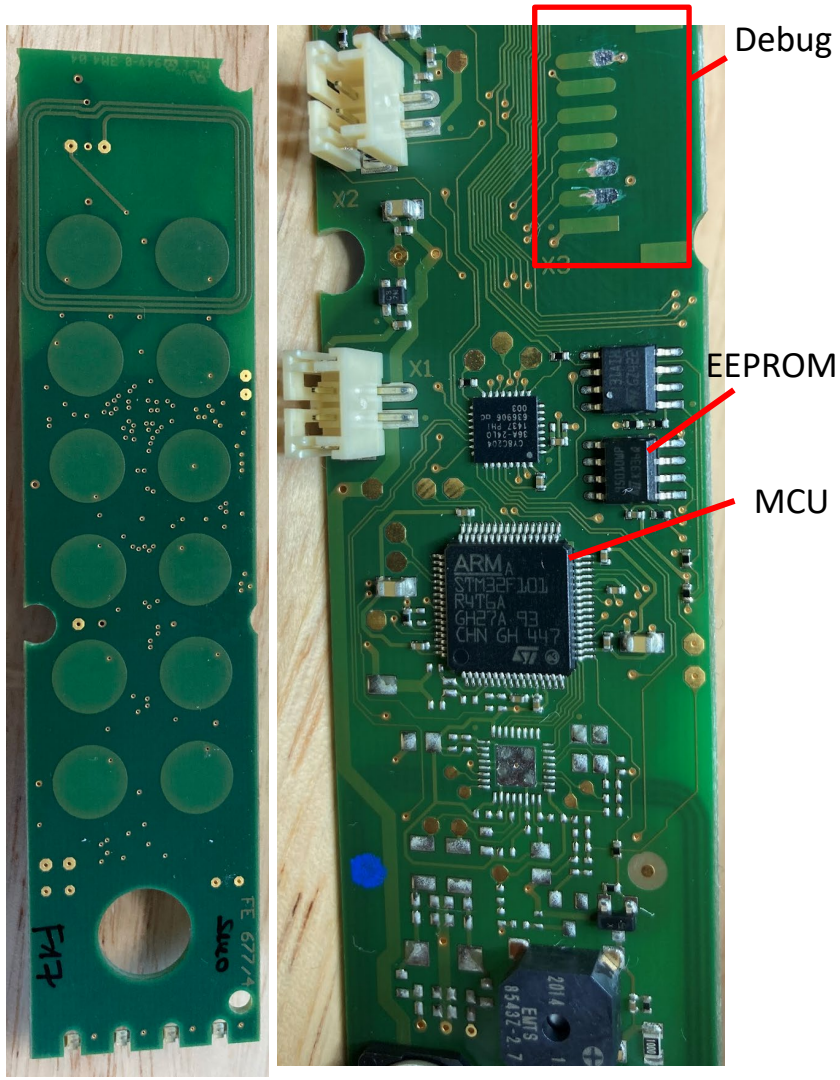
    * We do not cover door locks, but assume that they are the same platform as the cabinet locks
- Electronic locks
  - PIN, RFID, RFID+PIN
  - Audit logging supported

Disassembled SAG LS-100

Source(March 2024): https://en.sag-schlagbaum.com/company/history/

SAG LS-series locks

- Based on
  - STM32F101 MCU*
  - SPI EEPROM
- Security
  - SWD/Debugging not disabled
  - EEPROM not encrypted
  - No physical tamper switches

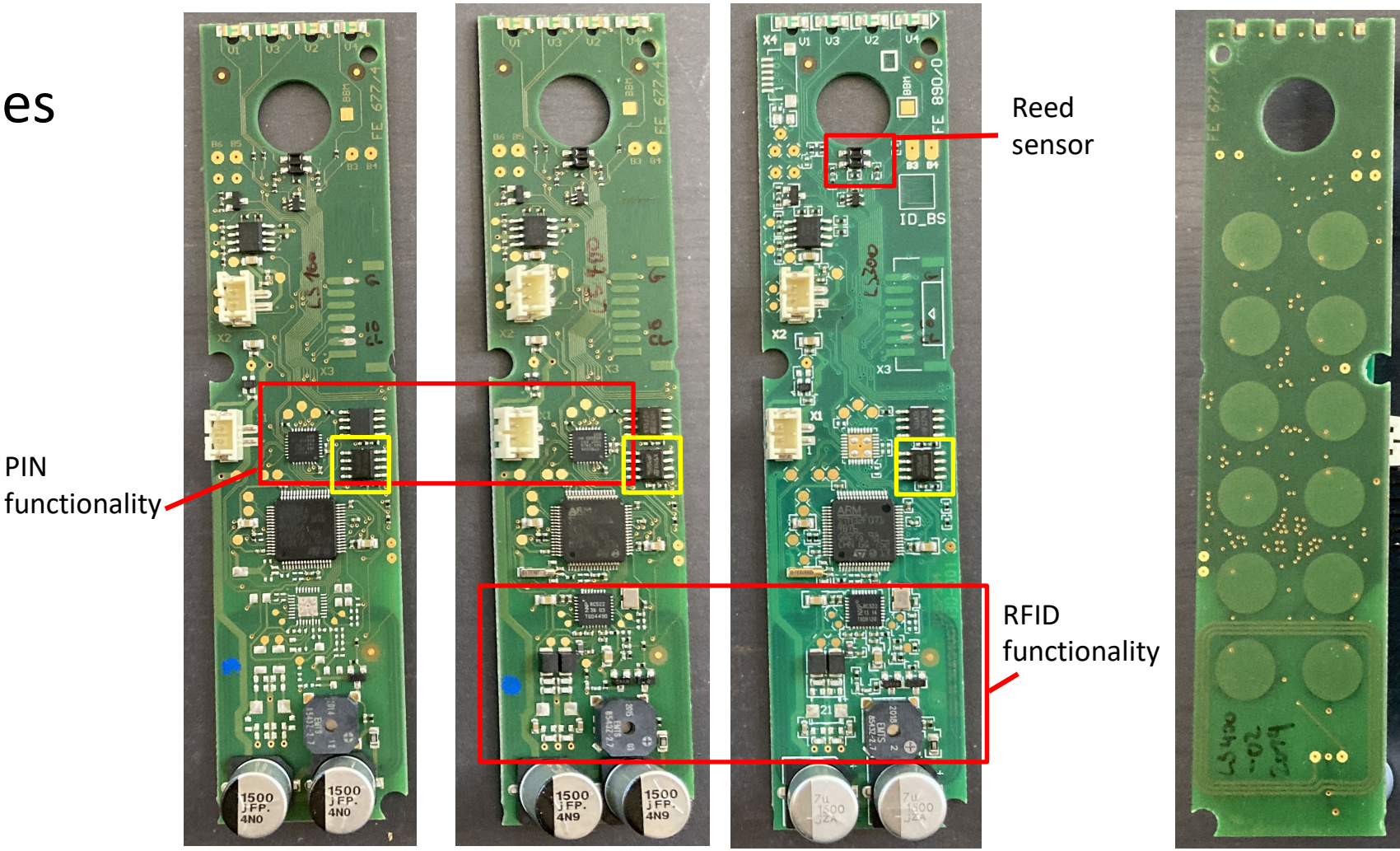


SAG LS-100 PCB

* recently, SAG switched from F101 (Cortex-M3) to F030 (Cortex-M0)

SAG LS-series locks

- Same PCB for all series
  - ICs unpopulated
- MCU for keypad
  - CY8C20436A
- MCU for RFID
  - NXP RC522
- SPI EEPROM size
  - PIN-only: 1kbit
  - RFID: 256kbit



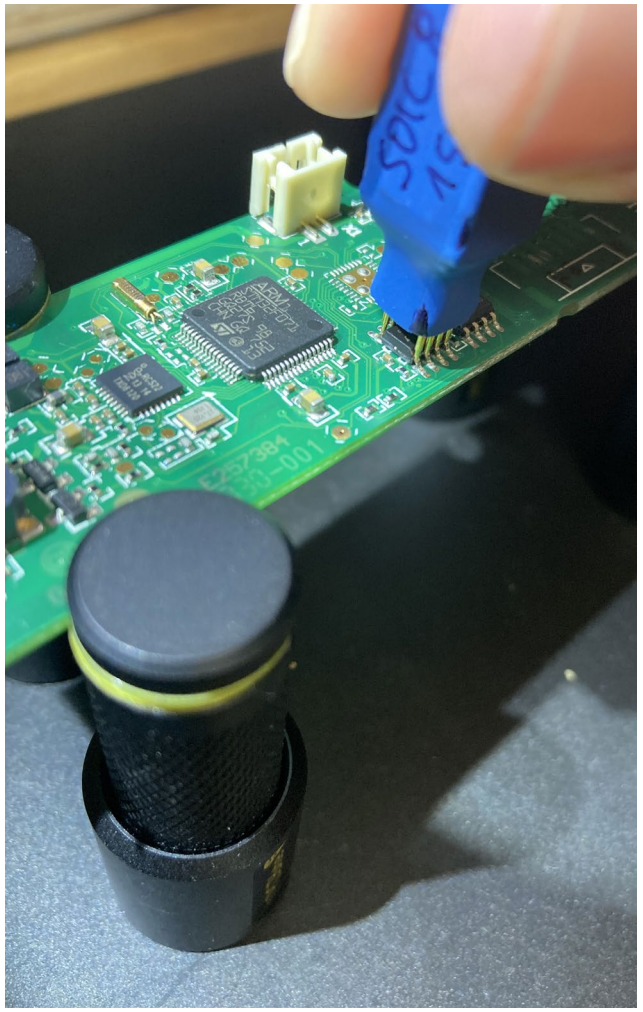
LS100 – PIN only | LS400 – PIN+RFID | LS300 – RFID only

SAG LS-series keys

- RFID: support for Mifare Classic, Mifare DESFIRE, ISO14443A
- For > LS100: special RFIDs keys required for programming
  - Master key I and II for unlocking/relocking lockers
  - “Data” RFID tag for data transport (e.g. audit logs)
  - “Communicator”: advanced handheld programmer

Screenshot/Source:
https://www.hafele.com/us/en/product/safe-o-tronic-ls200-programming-key-set-plastic-black-26mm-diameter/23198508/

SAG LS-series EEPROM contents



Access to SPI EEPROM via pogo pins

t	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00	1C	AF	CC	15	01	01	02	04	20	15	00	01	11	00	30	15
10	FE	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	14	04
20	10	02	03	00	01	01	11	83	00	00	01	37	48	00	AE	1D
30	00	00	FF	3C	3C	00	00	00	00	00	00	00	00	00	9B	19
40	00	02	00	00	00	00	00	00	00	01	33	70	00	00	CE	06
50	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
60	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

PIN

Master PIN

Fully provisioned LS-100 lock,
Master PIN “13370”,
PIN “3748” set

SAG LS-series EEPROM contents

- 500 entries

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000067B0	10	01	FE	E2	00	00	00	00	00	00	00	00	00	00	00	01
000067C0	10	01	FE	E2	14	04	00	00	00	00	12	34	00	00	00	50
000067D0	10	01	FD	E0	00	00	00	00	00	00	00	00	00	00	00	02
000067E0	10	01	FD	DF	14	04	00	00	00	00	12	34	00	00	00	50
000067F0	10	01	FD	CA	00	00	00	00	00	00	00	00	00	00	00	03
00006800	10	01	FD	C5	14	04	00	00	00	00	12	34	00	00	00	50
00006810	10	01	FD	AD	00	00	00	00	00	00	00	00	00	00	00	01
00006820	10	01	FD	AD	32	80	63	89	3A	CA	55	04	00	01	00	50
00006830	10	01	FD	A8	00	00	00	00	00	00	00	00	00	00	00	02
00006840	10	01	FD	A7	32	80	63	89	3A	CA	55	04	00	01	00	50
00006850	10	01	FD	9E	00	00	00	00	00	00	00	00	00	00	00	01
00006860	10	01	FD	9D	32	80	63	89	3A	CA	55	04	00	01	00	50
00006870	10	01	FD	9C	00	00	00	00	00	00	00	00	00	00	00	02
00006880	10	01	FD	99	32	80	63	89	3A	CA	55	04	00	01	00	50
00006890	10	01	FC	F4	00	00	00	00	00	00	00	00	00	00	00	01
000068A0	10	01	FC	F4	14	04	00	00	00	00	13	37	00	00	00	50
000068B0	10	01	FA	28	00	00	00	00	00	00	00	00	00	00	00	02
000068C0	10	01	FA	27	14	04	00	00	00	00	13	37	00	00	00	50

Status code

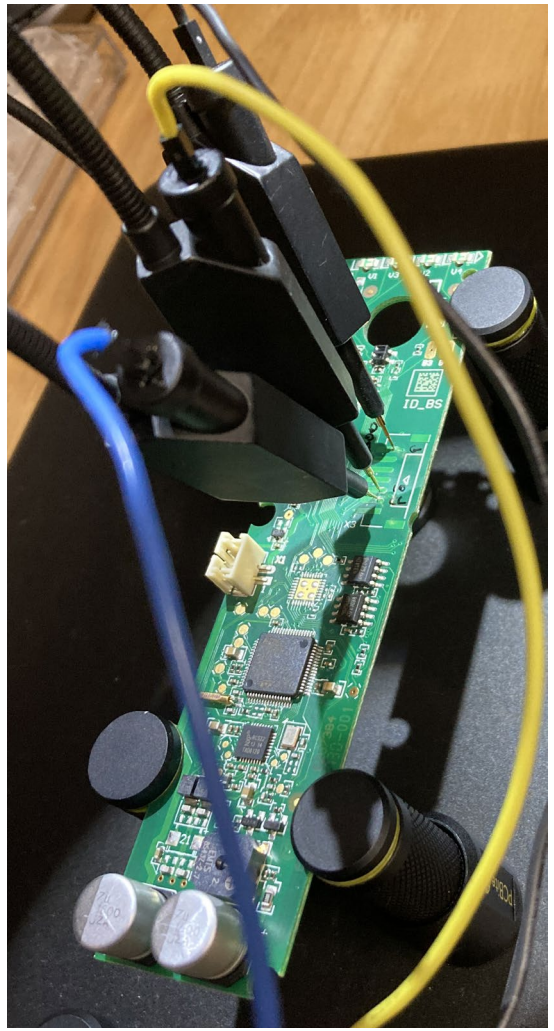
Timestamp

RFID UID

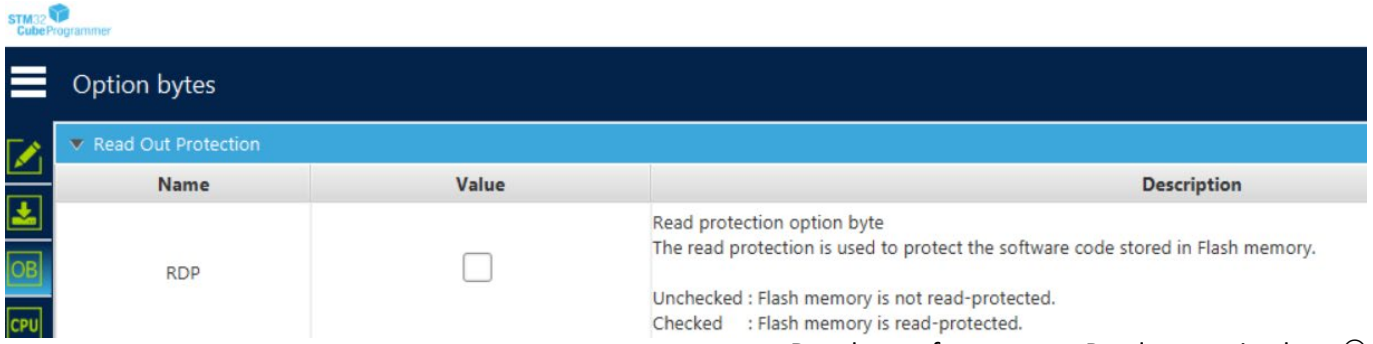
Used PIN

Fully provisioned LS-400 lock, audit logs enabled, RTC disabled

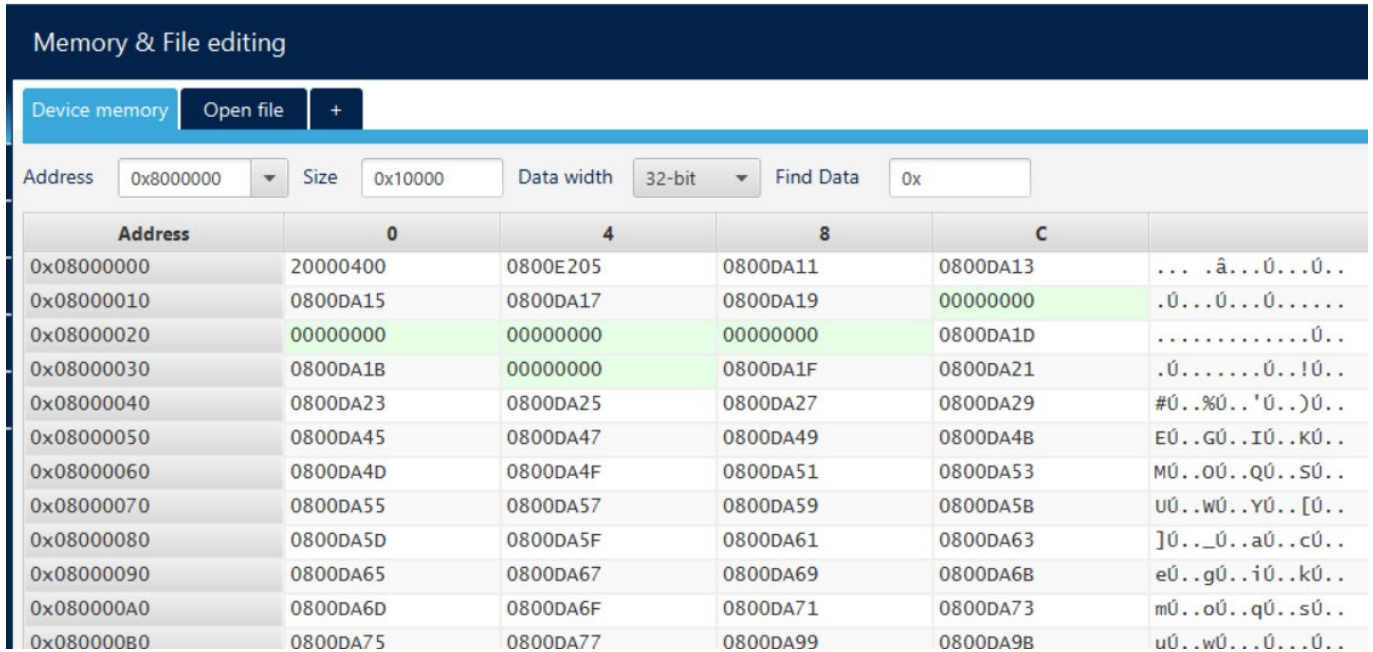
SAG LS-series extracting firmware



SWD debugging access with PCBites



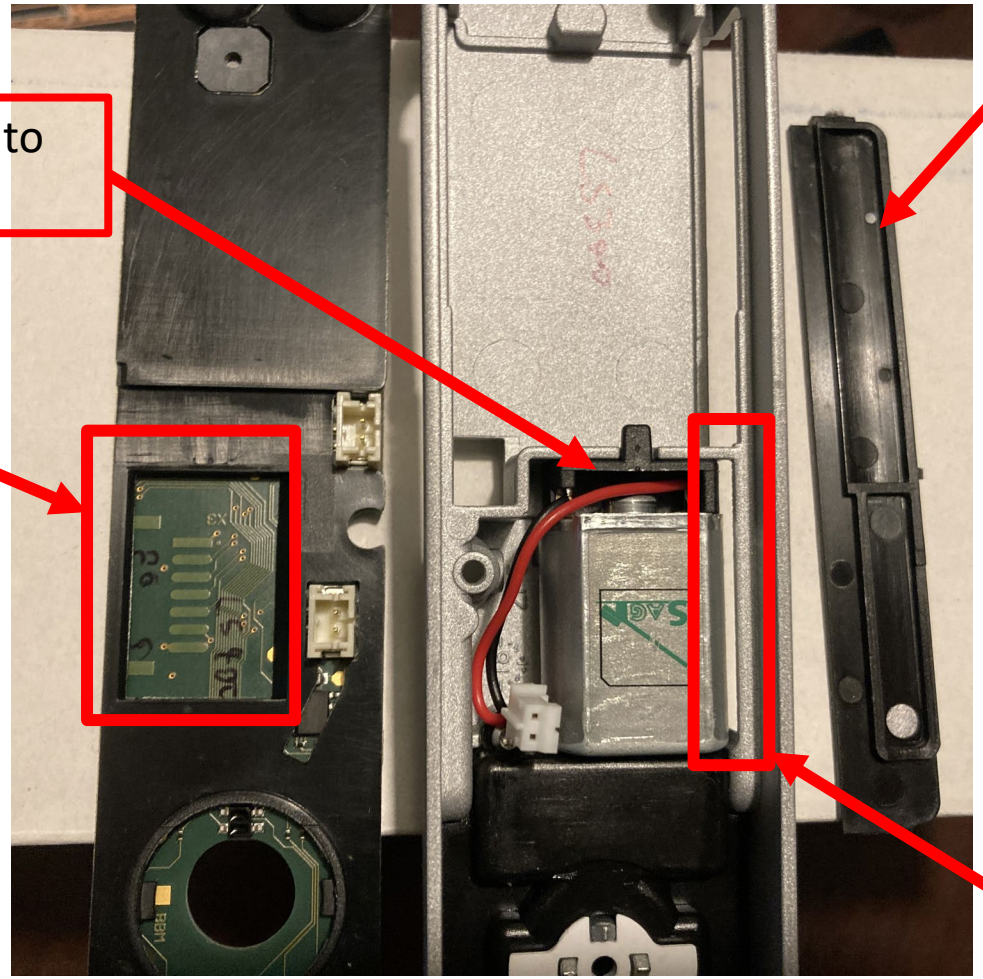
Developers forgot to set Read protection byte ☹

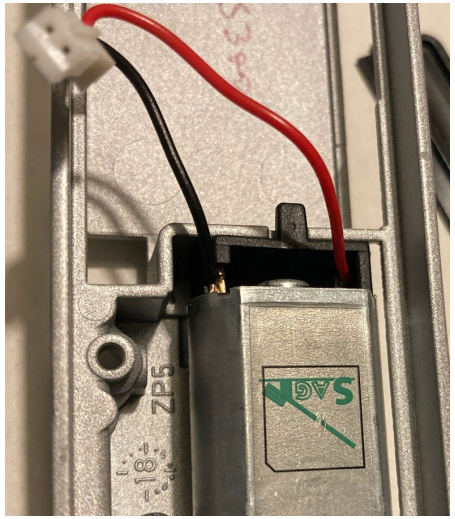


Address	0	4	8	C	
0x08000000	20000400	0800E205	0800DA11	0800DA13	... .â...Ú...Ú..
0x08000010	0800DA15	0800DA17	0800DA19	00000000	.Ú...Ú...Ú.....
0x08000020	00000000	00000000	00000000	0800DA1D	.....Ú..
0x08000030	0800DA1B	00000000	0800DA1F	0800DA21	.Ú.....Ú..!Ú..
0x08000040	0800DA23	0800DA25	0800DA27	0800DA29	#Ú..%Ú..'Ú..)Ú..
0x08000050	0800DA45	0800DA47	0800DA49	0800DA4B	EÚ..GÚ..IÚ..KÚ..
0x08000060	0800DA4D	0800DA4F	0800DA51	0800DA53	MÚ..OÚ..QÚ..SÚ..
0x08000070	0800DA55	0800DA57	0800DA59	0800DA5B	UÚ..WÚ..YÚ..[Ú..
0x08000080	0800DA5D	0800DA5F	0800DA61	0800DA63	]Ú.._Ú..aÚ..cÚ..
0x08000090	0800DA65	0800DA67	0800DA69	0800DA6B	eÚ..gÚ..iÚ..kÚ..
0x080000A0	0800DA6D	0800DA6F	0800DA71	0800DA73	mÚ..oÚ..qÚ..sÚ..
0x080000B0	0800DA75	0800DA77	0800DA99	0800DA9B	uÚ..wÚ...Ú...Ú..

Firmwaredump (in STM32 CubeProgrammer)

Physical flaws

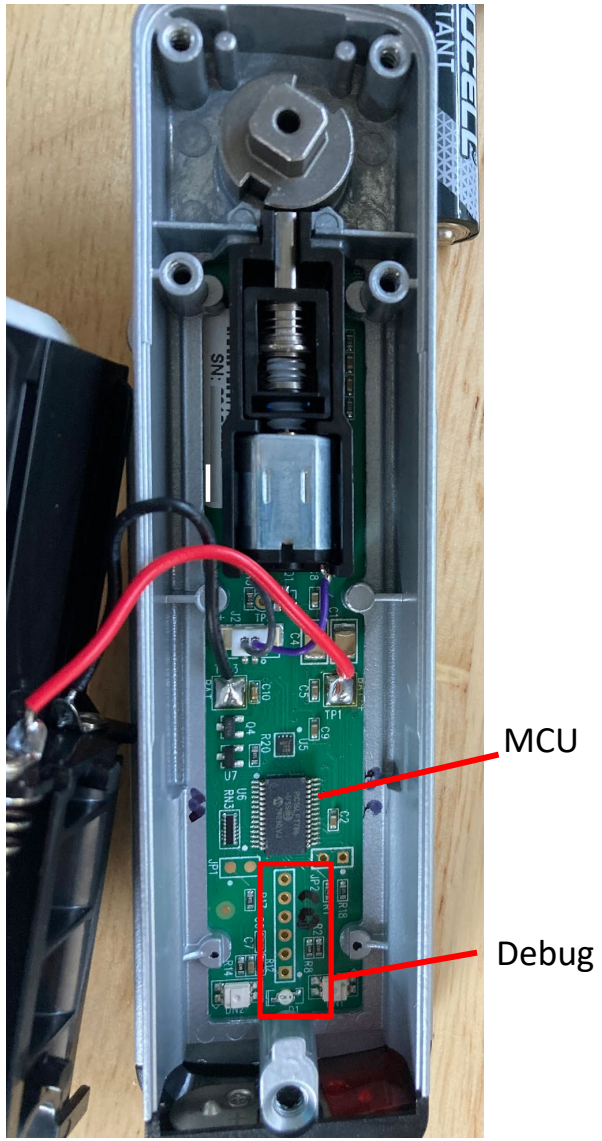




OTHER MANUFACTURERS

CompX

- “CompX Security Company”
- US company, founded in 1903
- RegulatoR Series
  - Based on PIC16LF
  - User PINs, Technician PINs, Master PIN
  - Audit logging for some models
- Security
  - Code, Data, Write protection enabled ☹

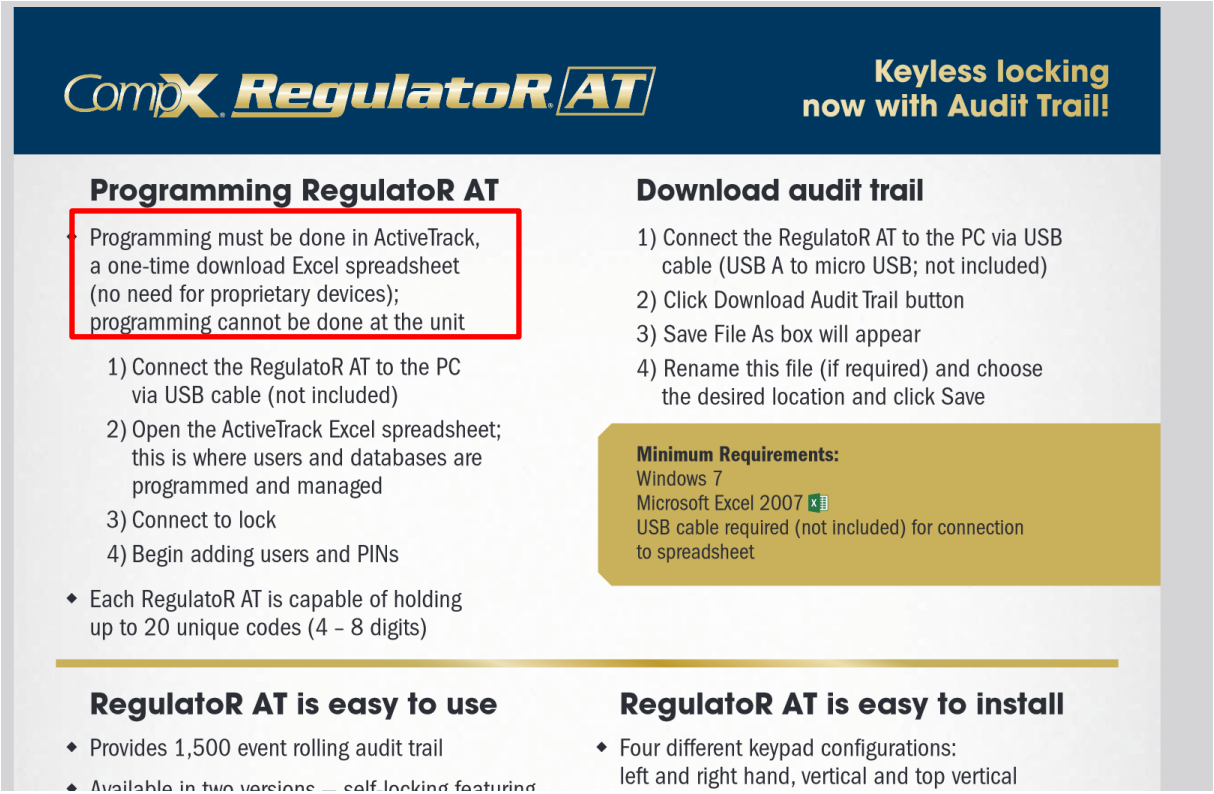


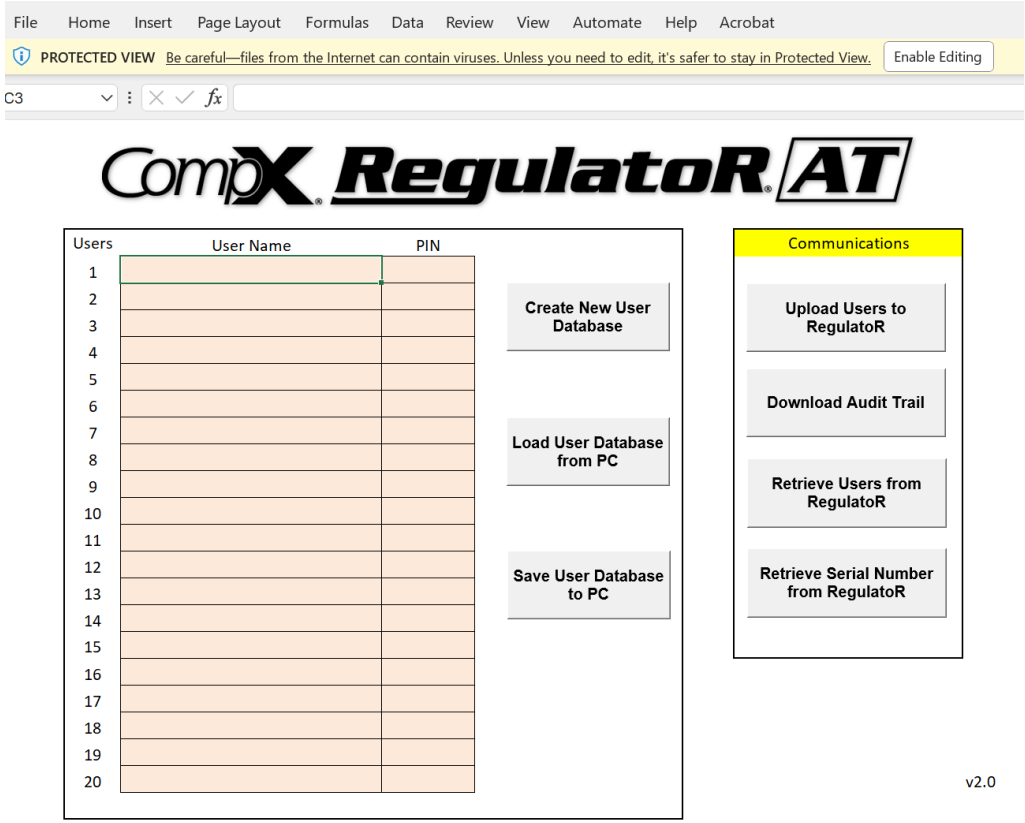
CompX Regulator Reg-SV3 (2016)

https://compx.com/brands/regulator/

CompX tool

- Programming/Audit tool: Excel Spreadsheet

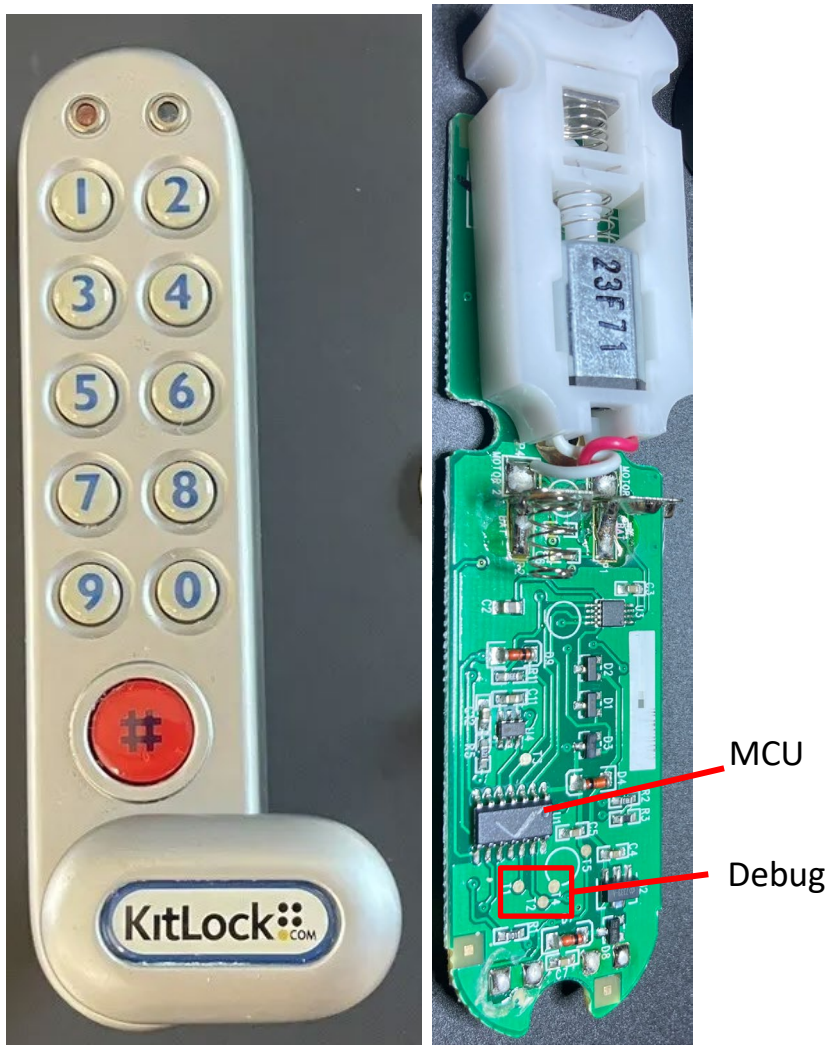




Source:
https://compx.com/product/regulator-at-self-locking-left-hand-7-16-reg-at-s-l-1/

Kitlock

- Brand of Codelocks
- UK based, founded in 1991
  - Based on PIC16LF
  - User PINs, Technician PINs, Master PIN
- Security
  - Code, Data, Write protection enabled ☹

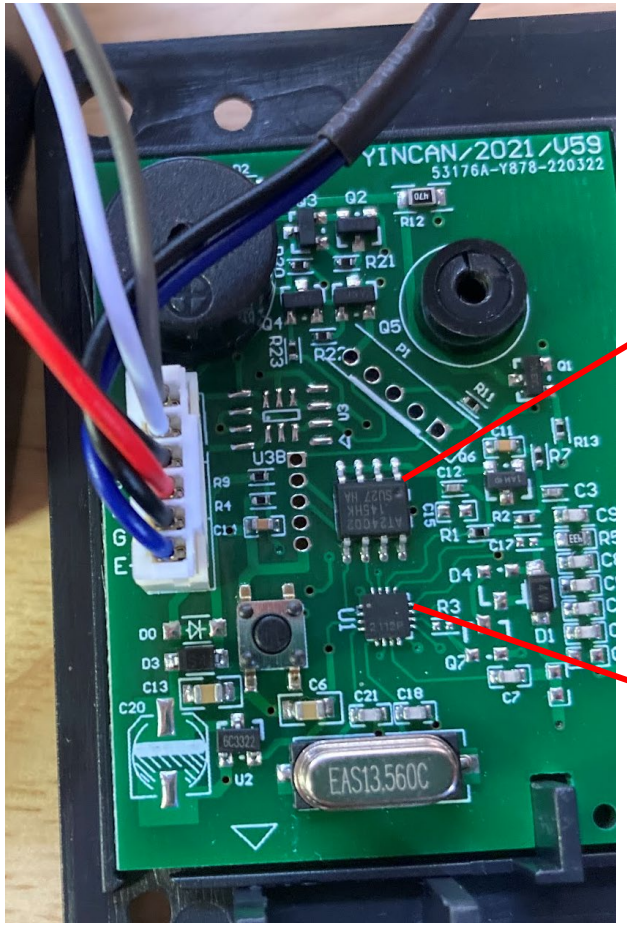


Kitlock KL1000

Noname RFID locks

- Cheap RFID locks on Amazon/eBay
- EEPROM and Mystery MCU
- No protection, plaintext RFID UIDs

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	00	00	00	00	23	FF	FF	FF	04	4C	01	85	23	FF	FF	FF
00000016	04	3E	FE	75	23	FF	FF	FF	04	B0	1E	81	23	FF	FF	FF
00000032	00	00	00	00	23	FF	FF	FF	00	00	00	00	23	FF	FF	FF
00000048	00	00	00	00	23	FF	FF	FF	00	00	00	00	23	FF	FF	FF
00000064	00	00	00	00	23	FF	FF	FF	00	00	00	00	23	FF	FF	FF
00000080	00	00	00	00	23	FF	FF	FF	00	00	00	00	23	FF	FF	FF
00000096	00	00	00	00	23	FF	FF	FF	00	00	00	00	23	FF	FF	FF
00000112	00	00	00	00	23	FF	FF	FF	00	00	00	00	23	FF	FF	FF
00000128	00	00	00	00	23	FF	FF	FF	00	00	00	00	23	FF	FF	FF
00000144	00	00	00	00	23	FF	FF	FF	00	00	00	00	23	FF	FF	FF
00000160	00	00	00	00	23	FF	FF	FF	00	00	00	00	23	FF	FF	FF
00000176	00	00	00	00	23	FF	FF	FF	00	00	00	00	23	FF	FF	FF
00000192	00	00	00	00	23	FF	FF	FF	00	00	00	00	23	FF	FF	FF
00000208	FF	FF	FF	FF	FF	FF	FF	FF	04	45	1E	A9	23	FF	FF	FF



DEMO

Example Scenario

- Assumption: Attacker has access to *any* open locker/cabinet
- Required tools: Debugger, Philips Screwdriver, Arduino/Flipper
- Goal: Clone Manager key, extract set user PIN/RFID UID

Demo

Find the recorded version of the demo here: https://dontvacuum.me/talks/DEFCON32-locks

CONCLUSION

Summary

- We can extract firmware and keys from Digilock/SAG locks
- Access to one lock can give you access to all (in one location)
- Cloning and emulating keys is possible
- Attacks do not require complicated tools and are cheap

how secure is your stuff in electronic lockers?

Not very secure!

Reminder: The locks are not sold as high-security locks!

Solutions

- Security-by-design from the beginning:
  - enable all security features, expect physical attacks
  - store secrets in a secure way
- Best solution for vulnerable locks: firmware updates for existing locks
- Problem: depending on age, existing locks likely unfixable
  - workaround: use programmer to enable code protection
    - only works if data is stored on the MCU
    - too complicated for average user (but might be solved by vendor)
- Likely: buy new locks or just ignore the problem

Take away lessons

- Do not re-use an important PIN for lockers/cabinets/safes !!!
- Never loan your electronic keys
- Be aware about the security limitations of these devices
- Do not trust audit logs of devices
- Even experienced and big companies make mistakes
- Producing a high-security but cheap system is difficult
- There might be interesting cyber-physical systems around you

Do not forget the human factor! Just ask nicely for the key?

Final notes

- Please do not break into lockers you do not own!
- Messing with locks can permanently brick them
- There are more attacks that have not been covered here
- Other companies and products are vulnerable, too
  - Just because someone did not get hacked, does not mean that they are good

Special thanks:

Cory Doctorow
Tarah Wheeler
Hannah Zhao
Kurt Opsahl
Andrew Crocker
the legal team @EFF
https://supporters.eff.org/donate/join-eff

Contact:

See: http://dontvacuum.me
Telegram: https://t.me/dgiese
Twitter: dgi_DE
Email: dennis@dontvacuum.me
hi@braelynn.io

Acknowledgements:

@Tihmstar
Shannon Assouline
Ben Helfrich
Sören Beye
Gene Stephens
@AapoOksman
Xenia
Guevara Noubir

BACKUP SLIDES

Digilock full statement

Digilock respects Mr. Giese's research. Prior to DEFCON, Digilock and Mr. Giese had communicated about code improvement for Digilock's products.

Additional security implementations by Digilock to further protect the code include:

- Implementation of code protection on all data blocks to address issues mentioned in Mr. Giese's findings
- Preliminary changes made to implement code protection for all blocks (PIC18) and GSS (PIC24)
- Additionally, internal EEPROM on PIC18 read protection is enabled.
- Additional encryption is being implemented to ensure that key values are encrypted during communication. Even if raw key UID is acquired, communication checks will prevent the key from being cloned with this raw communication with the lock.
- EEPROM data encryption is being implemented to ensure that data at rest and in transit is encrypted. This encryption is being applied to models using PIC18 internal and PIC24 external EEPROM.

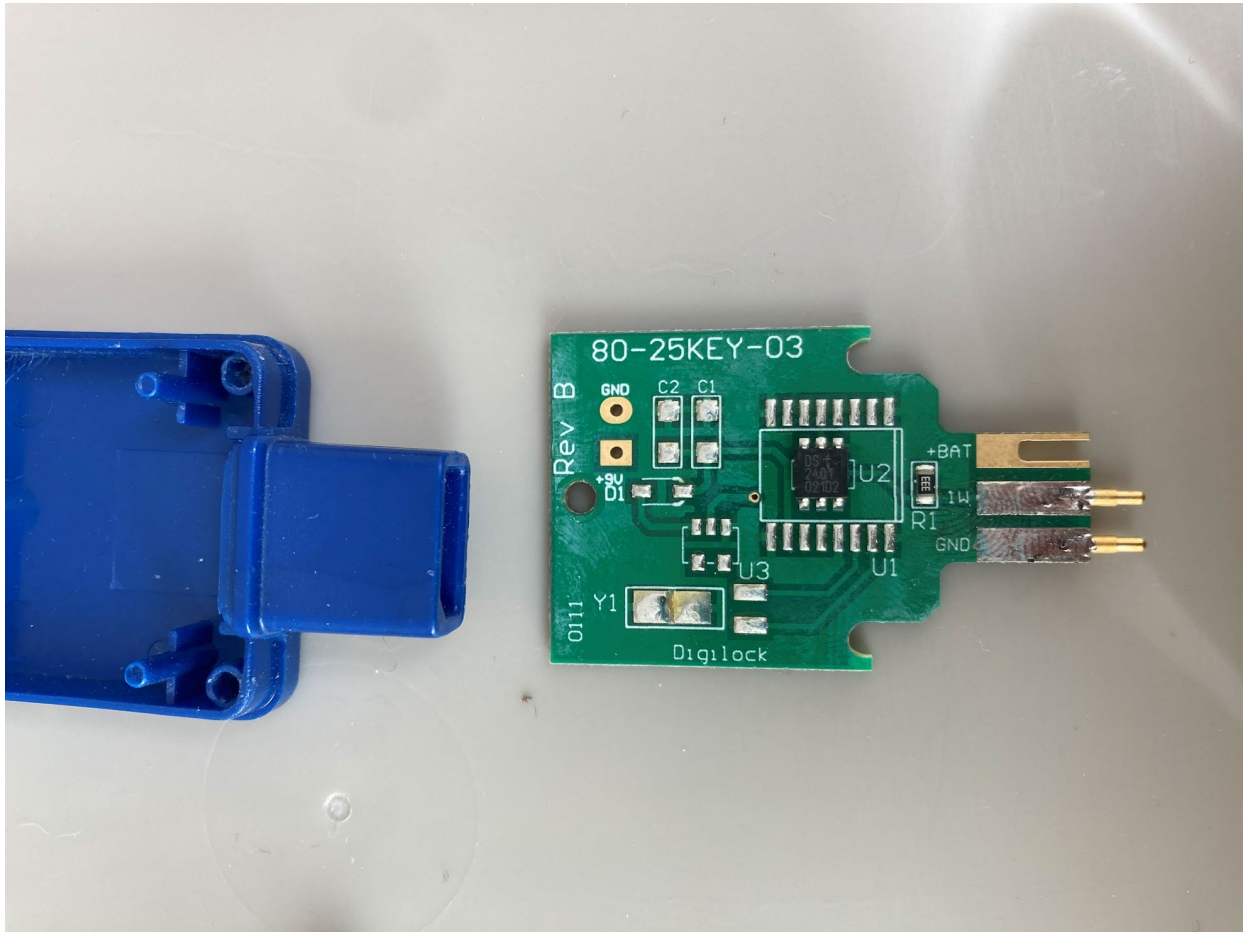
Digilock thanks Mr. Giese for delaying his DEFCON presentation a couple of days to allow Digilock and Mr. Giese more time to discuss such issues. Digilock and Mr. Giese hope to continue collaboration and improve lock security.

In over 32 years, there have been no reported instances of items being stolen because a Digilock lock was hacked, Digilock is fully committed to providing secure solutions for its customers.

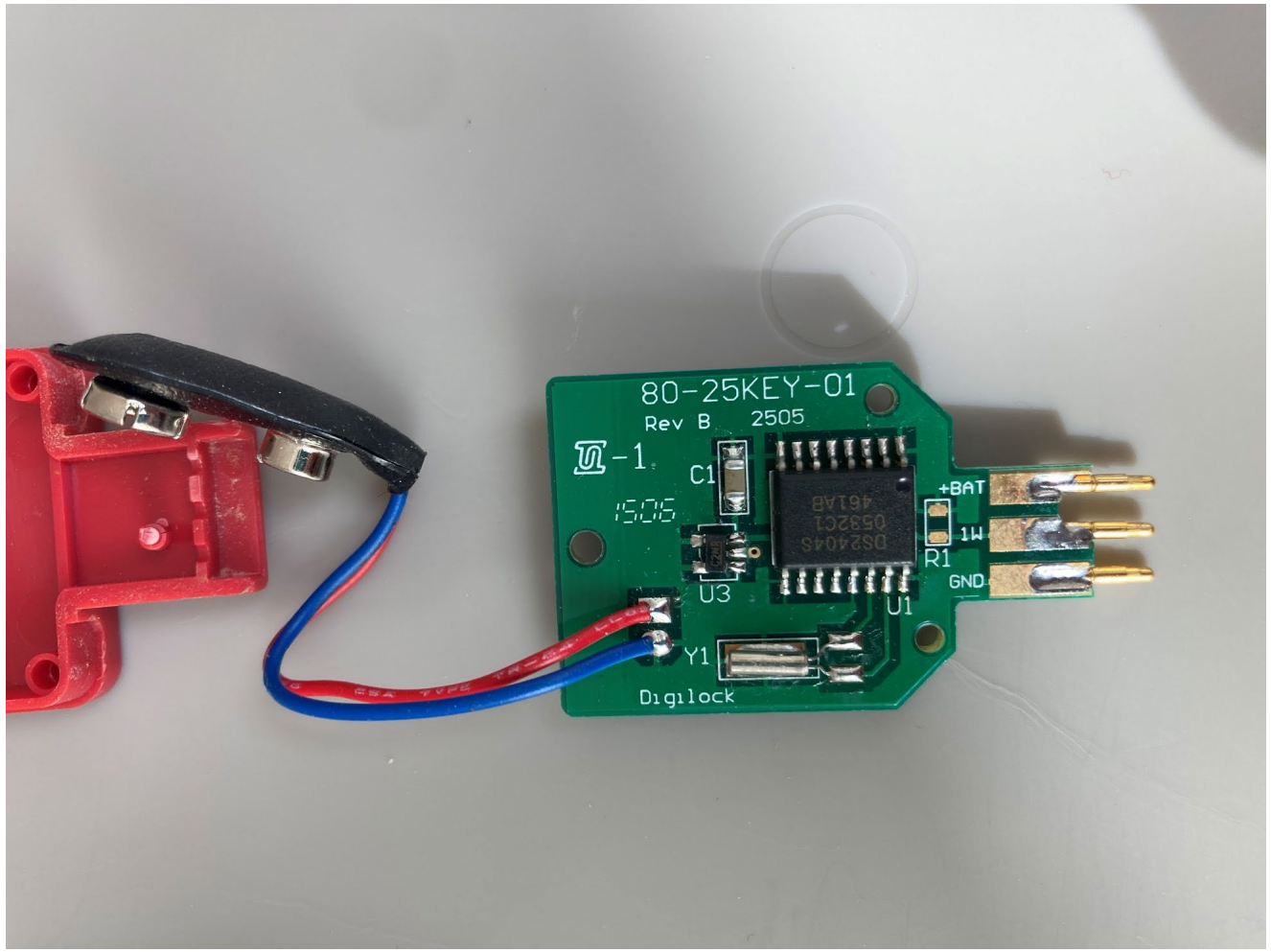
Devices under test

Model	SKU	MCU	EEPROM	PIN/Key location	CP	DP	WP	Pin erased after unlock	Year
ADA Key	Digilock 80-25KEY-03	DS2401+ (Serial 0x01)		-	-	-		-	2019
RED Key	Digilock 80-25KEY-01	DS2404S(ROM 0x04 + Time)		-	-	-		-	
4G Prog/Mgmt Key	Digilock 80-35KEY-05	PIC18F25K20-I/SO		-	Y(1-2)	N	N	-	2020
5G Prog/Mgmt Key	Digilock 80-35KEY-10 0617	PIC18F25K20-I/SO		-	Y(1-2)	N	N	-	
Data Key	Digilock 80-35DAK-12 1119	PIC24FJ64GA004	ST 24256BRP, MC 23K256	-	N	N (EP)	N	-	
4G RFID	Digilock 8050FAR-D1 0612	PIC24FJ64GA004	24LC02BISN	EP	N	N (EP)	N	N	2015
Numeris Versa Mini	Digilock 80-56VMFK-10 0621	PIC18LF46K40/MV		MCU-Data	N	N	N	Y	2022
NEXT AXIS	Digilock 80-60SSFK-03	PIC18F45K20	ST 24256BF TTSOP8	MCU-data	Y(1-2)	N	N	Y	2018
NEXT CUE	Digilock 80-36FLS-05	PIC18F25K20-I/SO		MCU-data	Y(1-2)	N	N	N	2017
NEXT AXIS vertical	Digilock 80-61SNFK-03	PIC18F45K20	ST 24256BF TTSOP8	MCU-data	Y(1-2)	N	N	Y	2019
4G	Digilock 80-50FAK-D2 Rev 1	PIC18F25K20-I/SO		MCU-data	Y(1-2)	N	N	N	2018
LS100	300841	STM32F101R4T6	ST M95010WP	EP	N	N (EP)	N	N	2016
LS300	300843	STM32F071RBT6	ST M95256WP	EP	N	N (EP)	N	N	2018
LS400	300844	STM32F101R4T6	ST M95256WP	EP	N	N (EP)	N	N	2015
KL1000		PIC16LF1825		MCU-data	Y	Y	N	-	
Regulator Reg-SV3		PIC16LF1786		MCU-data	Y	Y	Y	-	
RFID lock		2112P?	AT24002	EP		N (EP)			

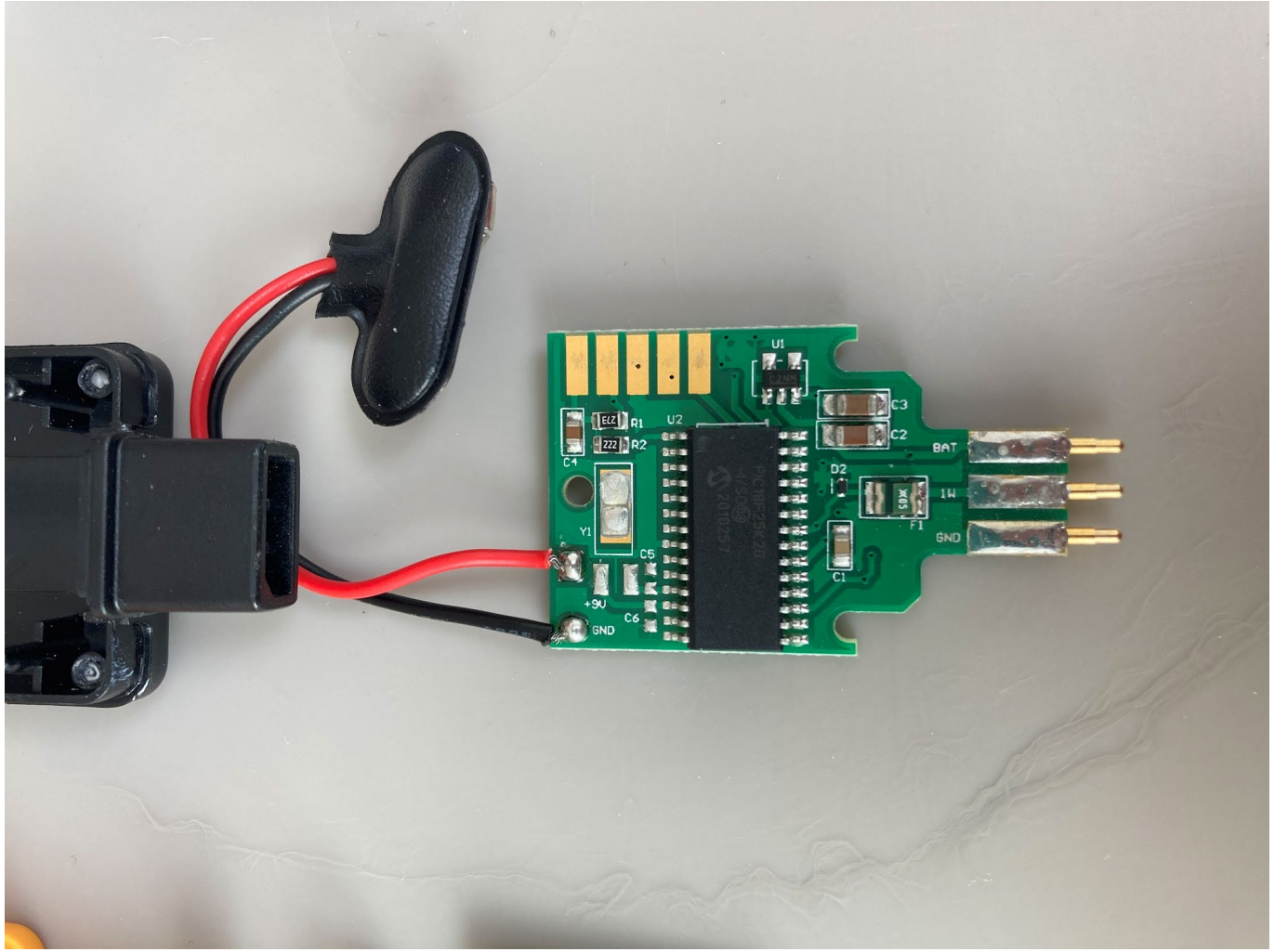
Digilock ADA Key



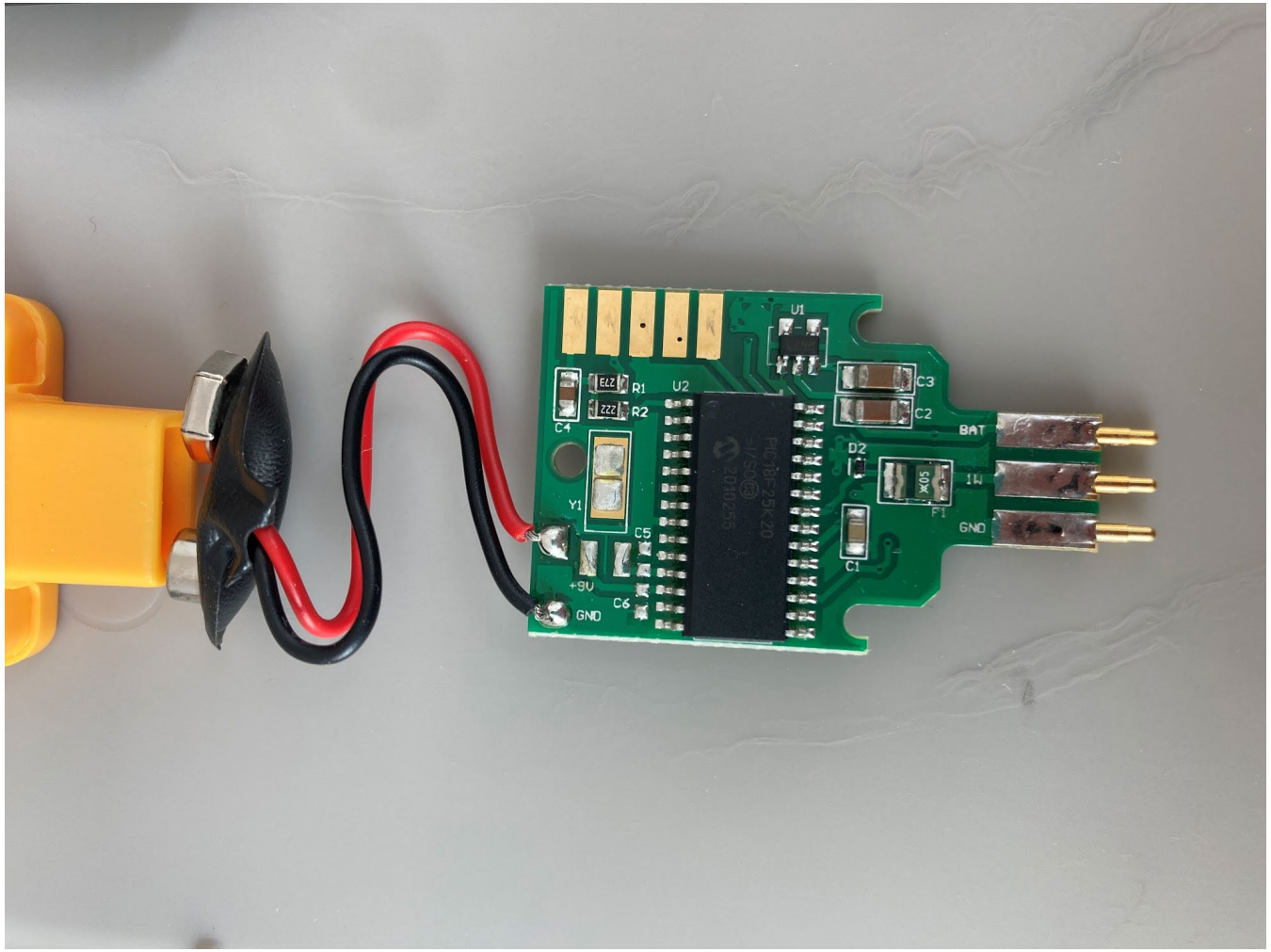
Digilock 3G Programming Key



Digilock 4G Manager Key



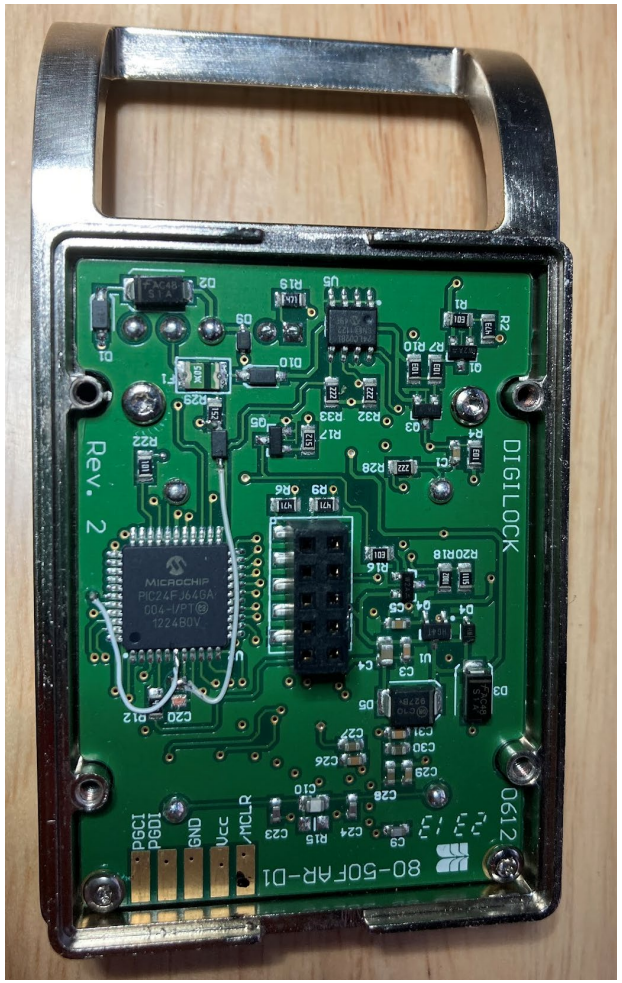
Digilock 4G Programming Key

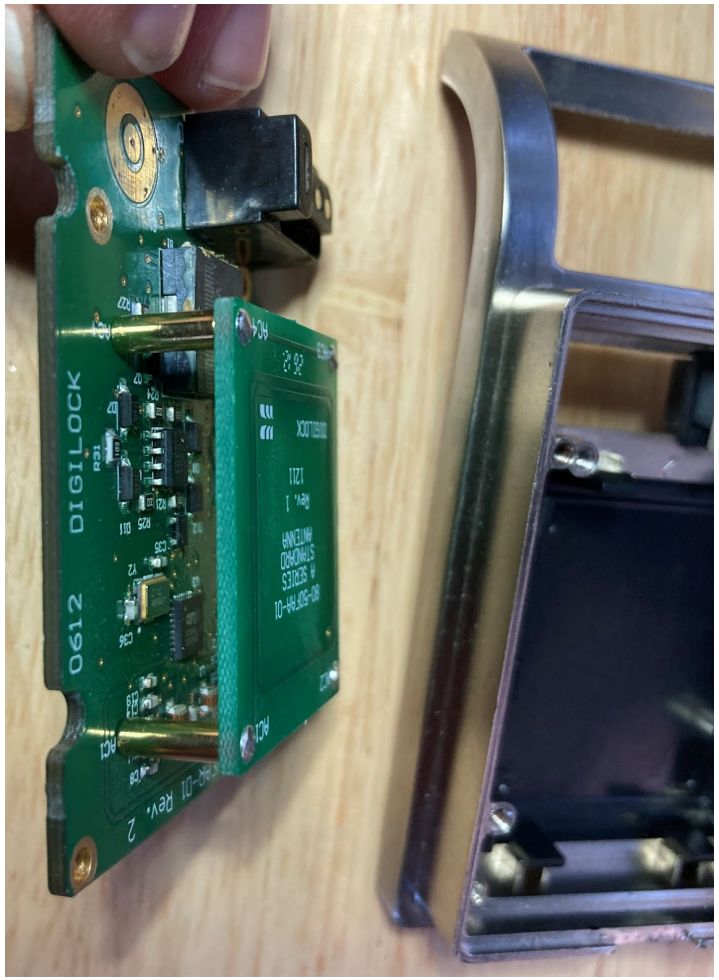


Digilock 5G Programming Key

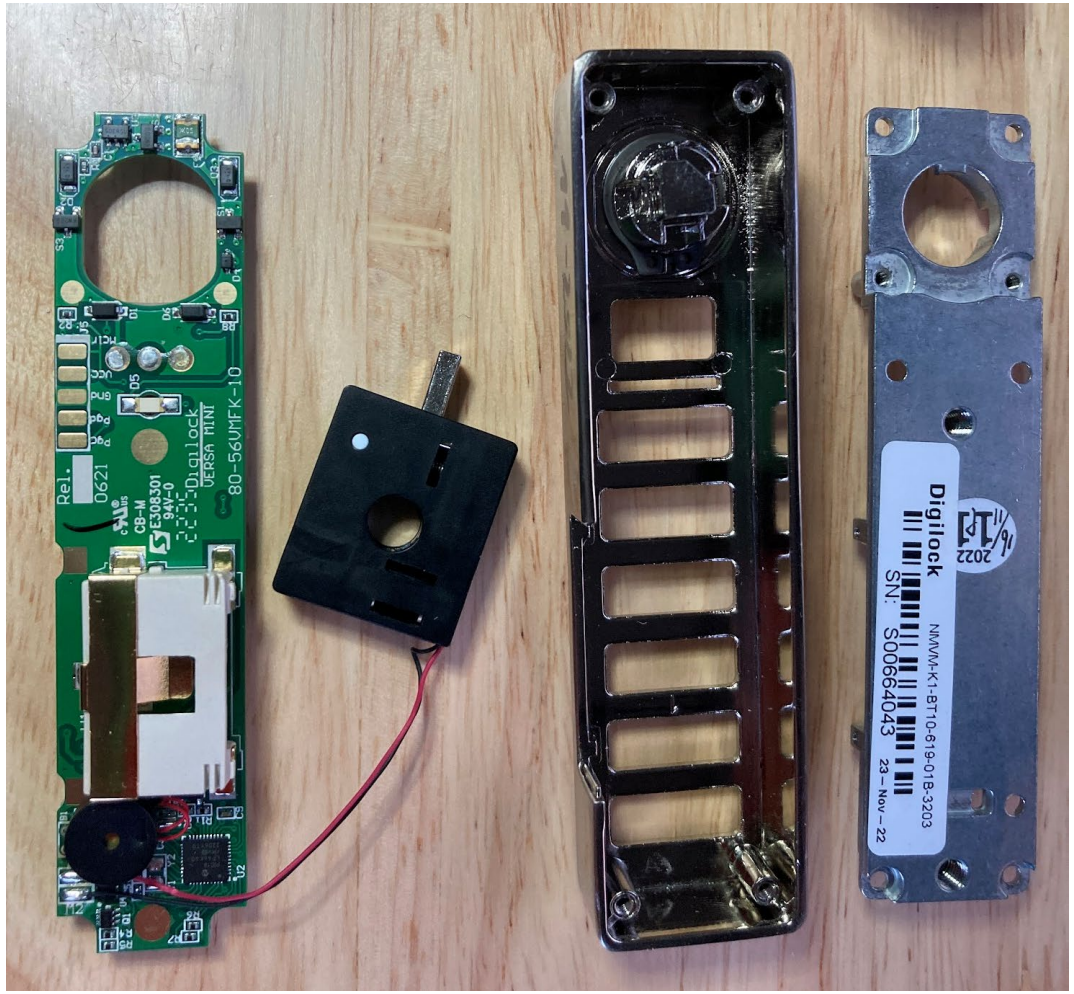
Digilock Data Key

Digilock 4G RFID

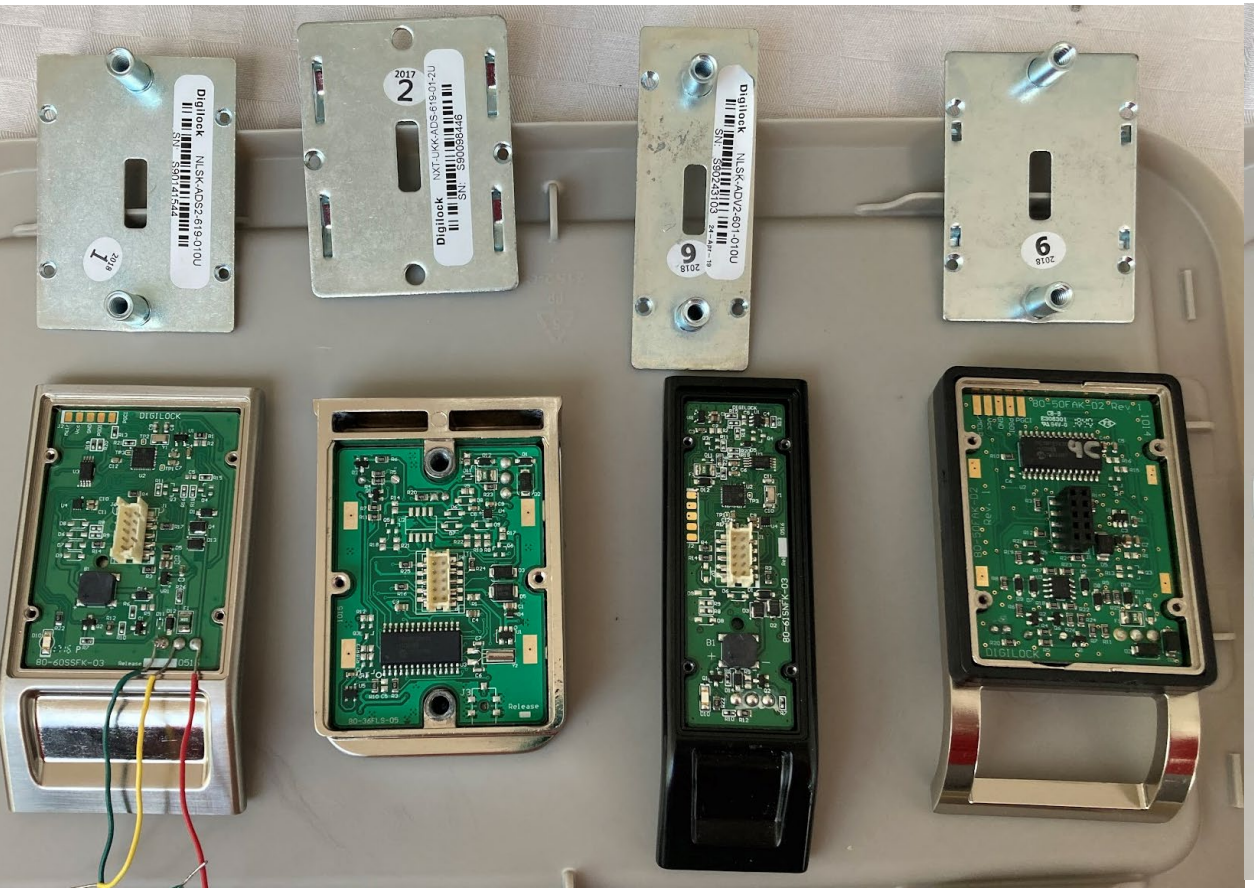


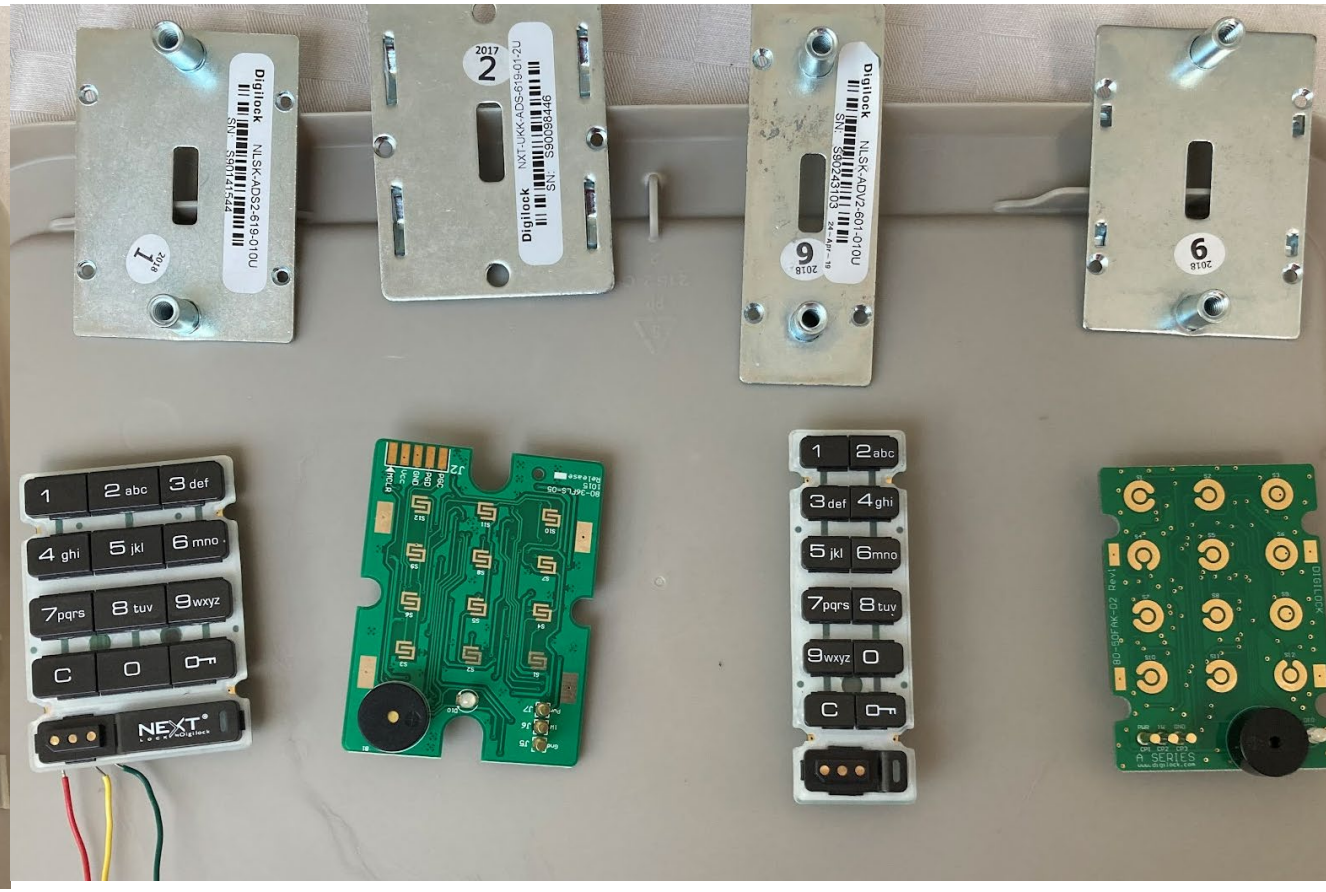


Digilock Versa Mini

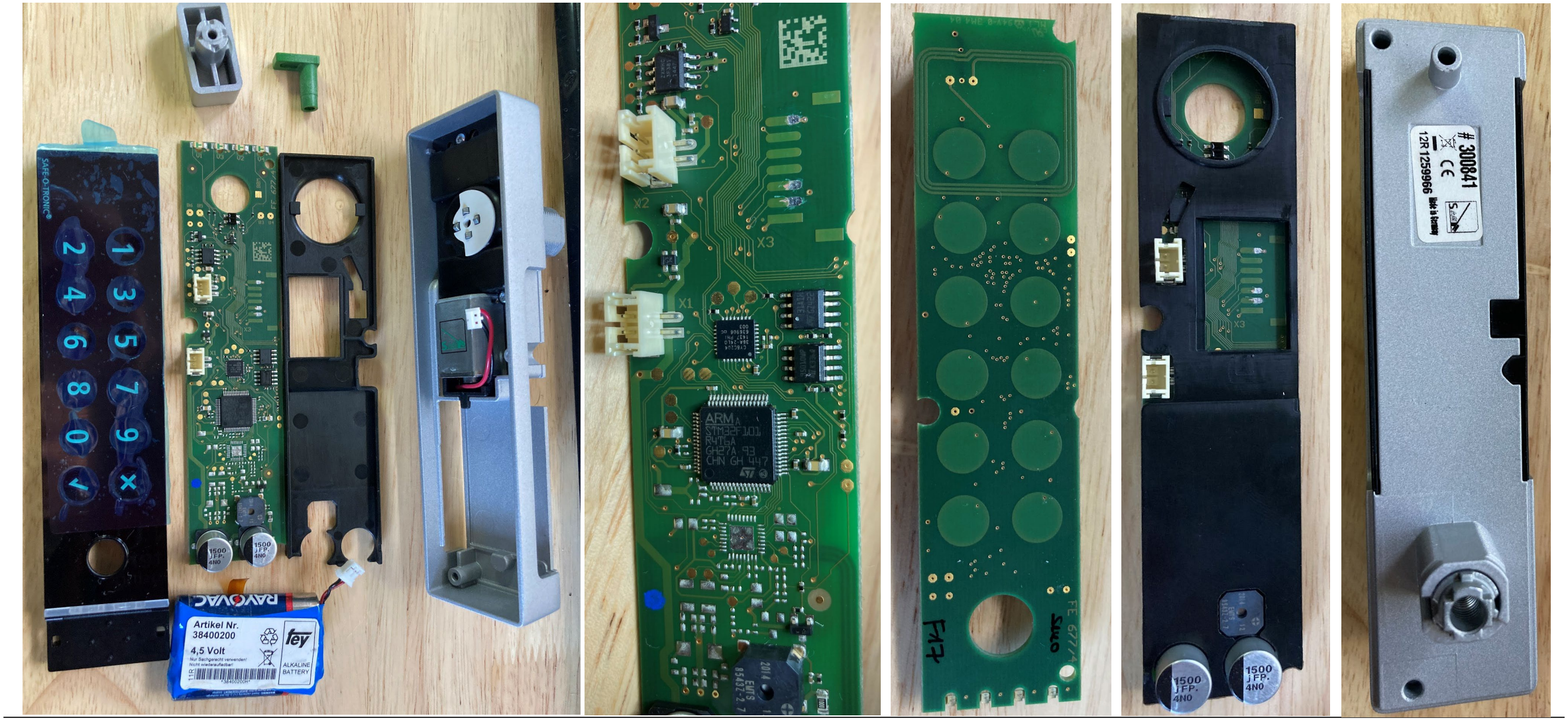


Digilock Axis/Cue/Axis/4G

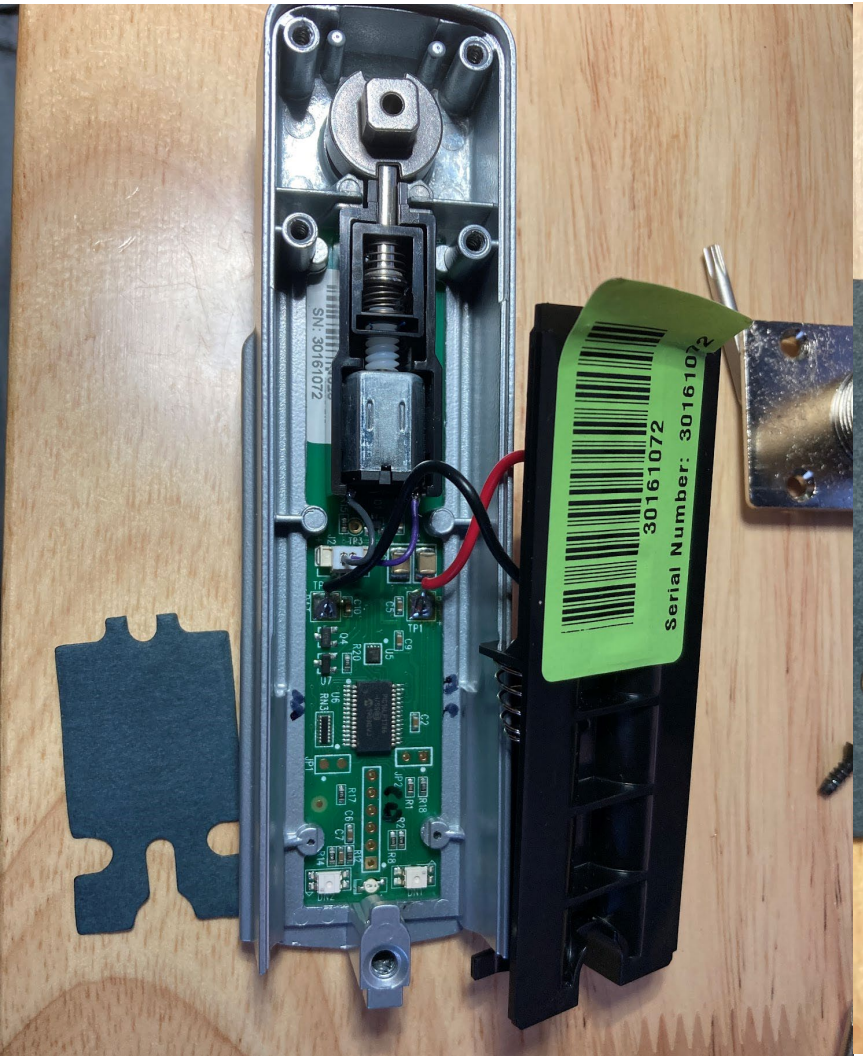


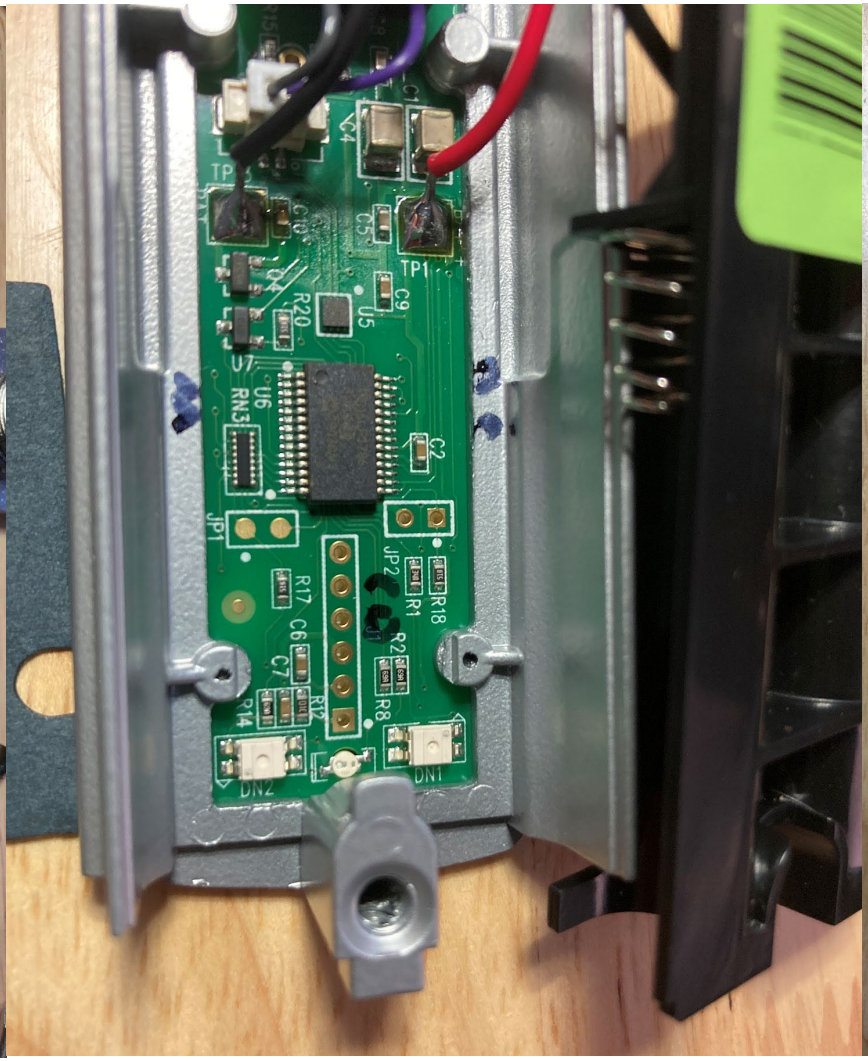


SAG LS100


SAFE-O-TRONIC
1500 µFP. 4N0
1500 µFP. 4N0
RAVOVAC
Artikel Nr. 38400200
4,5 Volt
fey
ALKALINE BATTERY
X2
X1
X3
ARM
STM32F101
R4T6A
GH27A 93
CHN GH 447
FE 677/1
1500 µFP. 4N0
1500 µFP. 4N0
300841
12R 1259966

CompX Lock


30161072
Serial Number: 30161072




30161072
Serial Number: 30161072

Kitlock