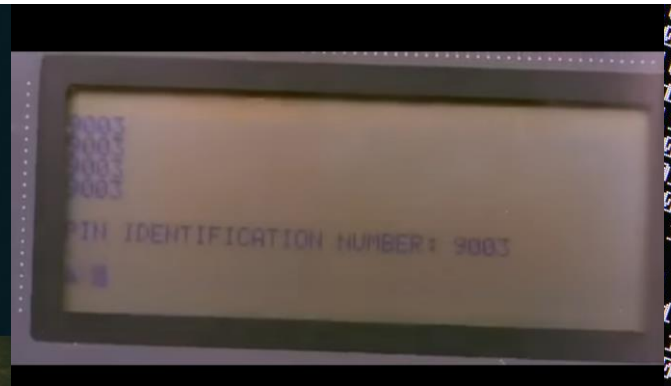
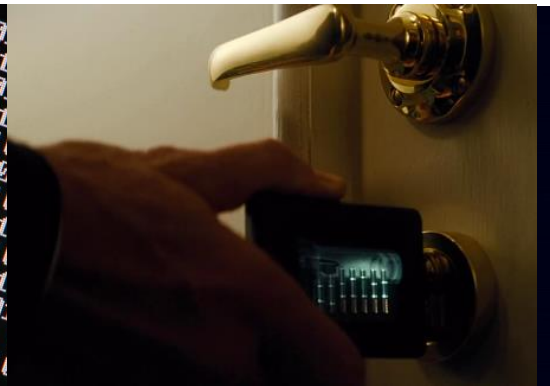
BREAKING ELECTRONIC LOCKS LIKE YOU'RE ON CSI: CYBER

Colin O'Flynn

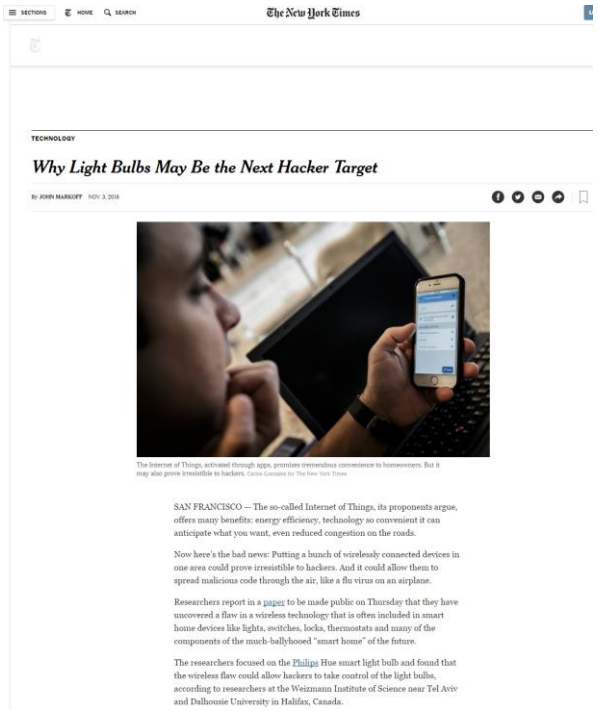




ABOUT ME

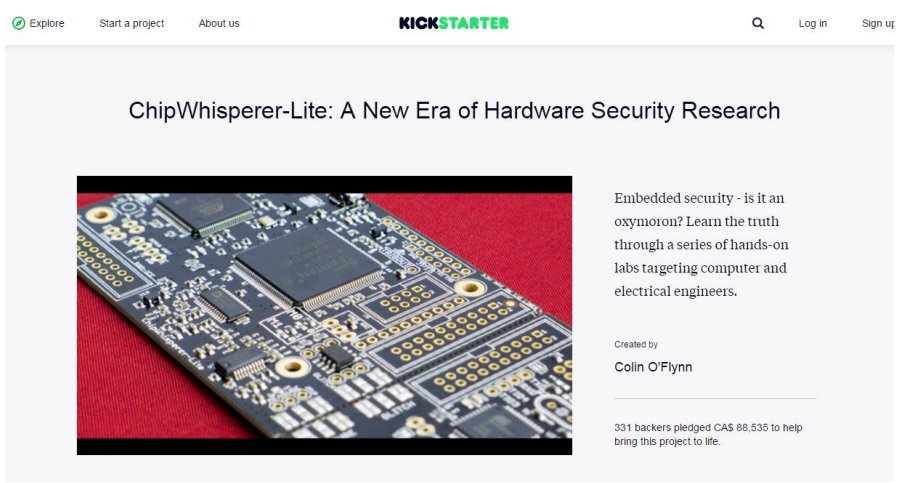
@Dalhousie University

- Recently finished PhD in Electrical Engineering.
- Various academic publications.
- Various conference presentations (Black Hat, DEFCON, etc).

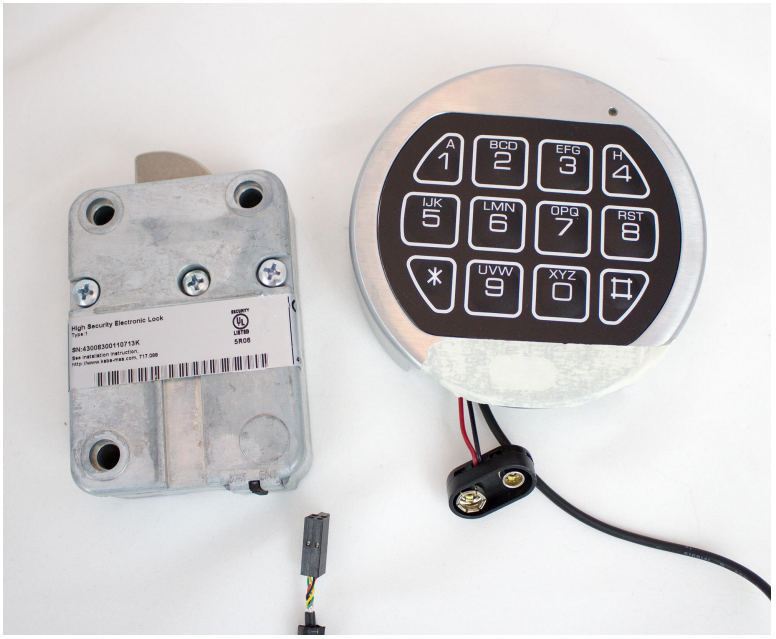


@NewAE Technology Inc.

- Launched Open-Source ChipWhisperer
- Variety of training, software, hardware around advanced embedded attacks.



ELECTRONIC LOCKS



THREAT VECTOR

Most Interesting (for me):

- Reprogram lock from frontside.
- Bypass Lock from frontside.

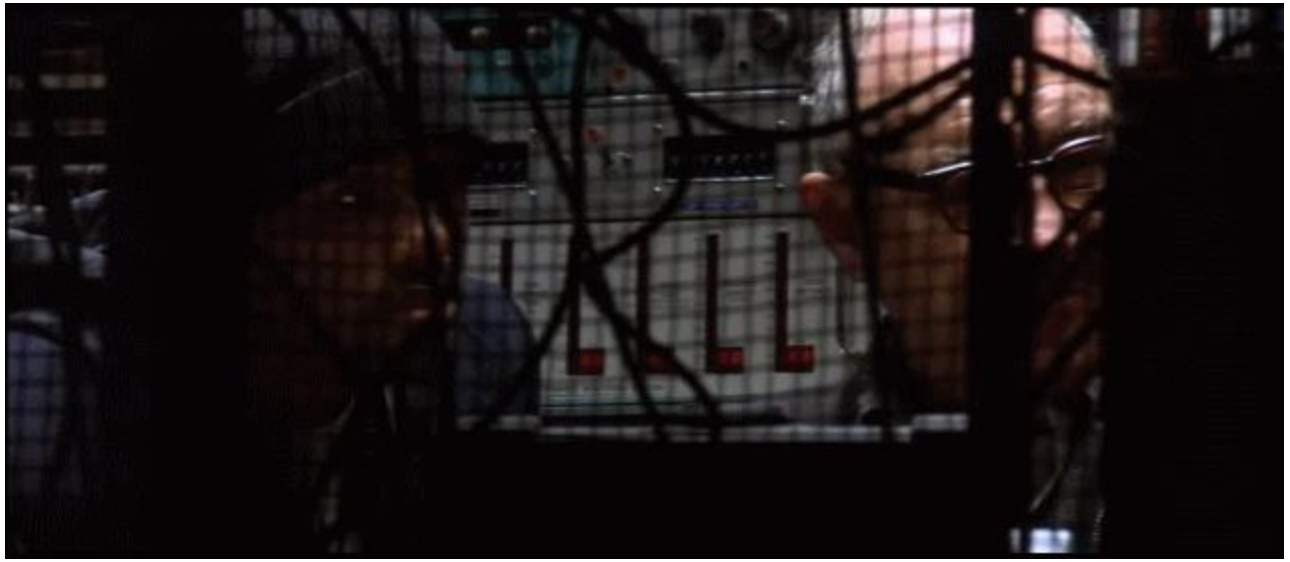
Less Interesting:

- Reprogram lock from inside (‘evil maid’).
- Mechanical attacks (lockpicking, etc).

NOTE ON VENDOR RESPONSE TO THIS

- Vendor was notified – they have been *extremely receptive* and are working on a fix, along with some general improvements beyond the one particular flaw (I have redacted full details for now on account of that).

BYPASSING LOCKS IN MOVIES

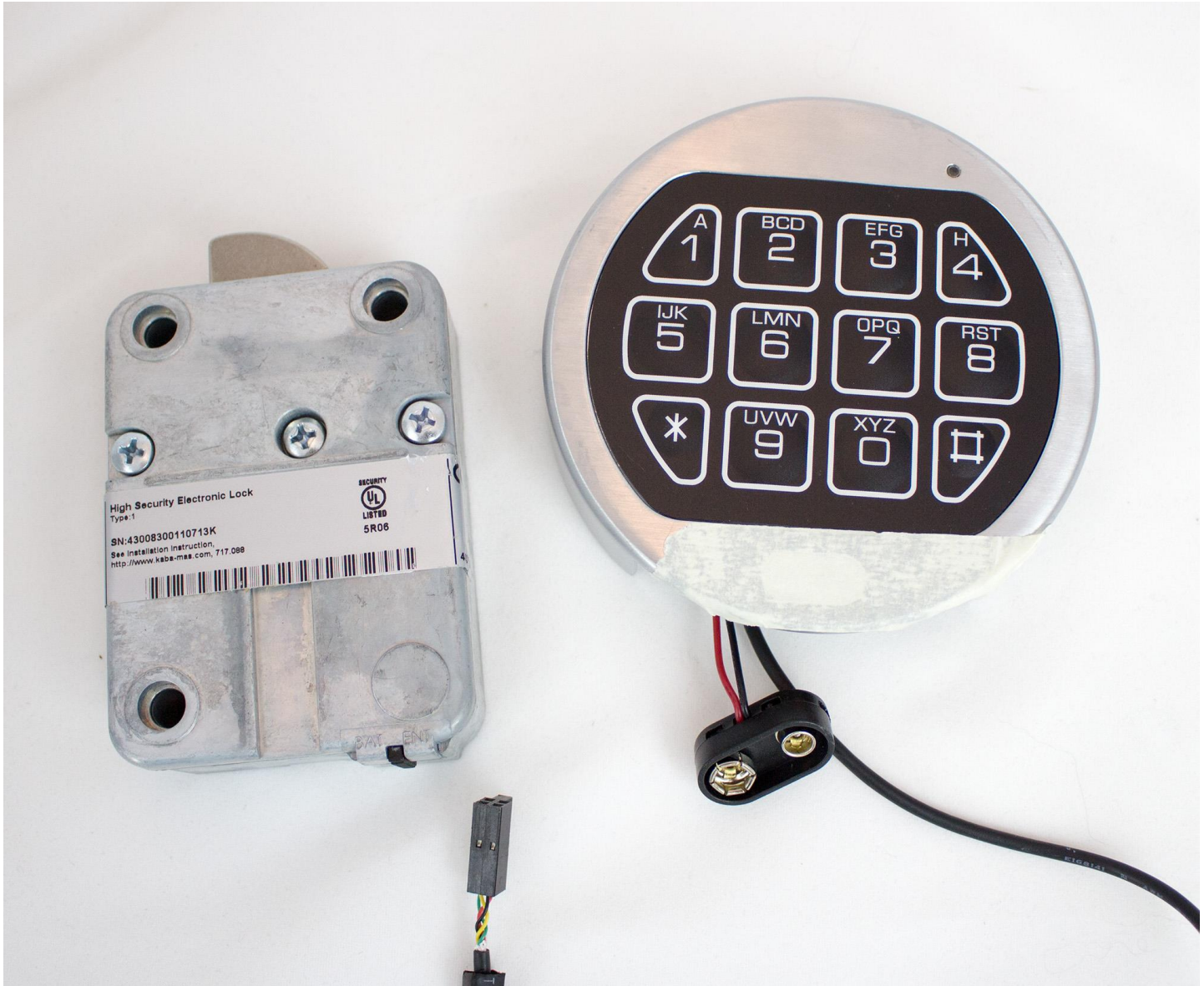


TYPES OF LOCKS I'VE LOOKED AT

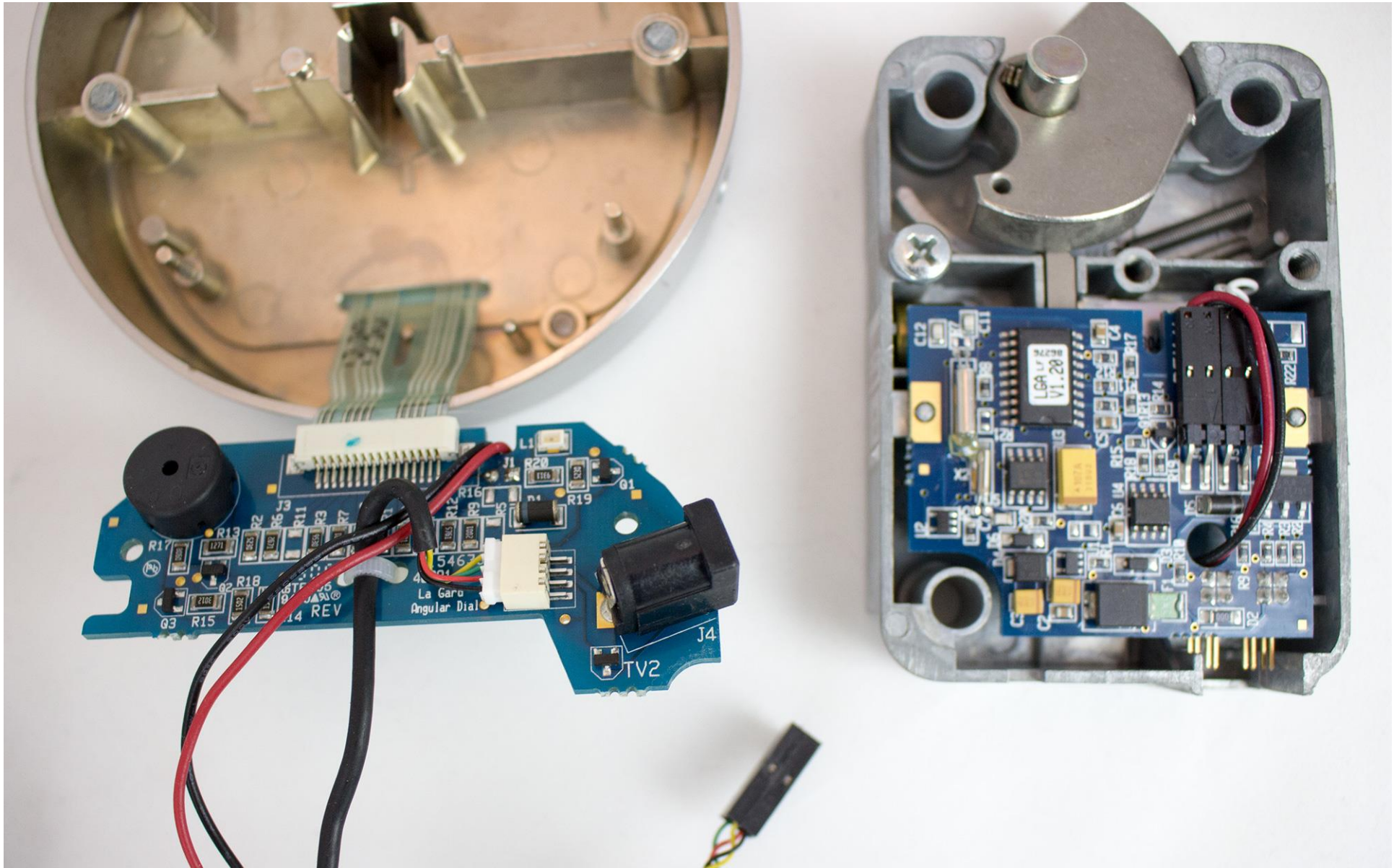
"High"-Security (Safe Keypad, $200-$1000)

Residential ($100-$300)

LOCK #1: HIGH-SECURITY, SAFE KEYPAD

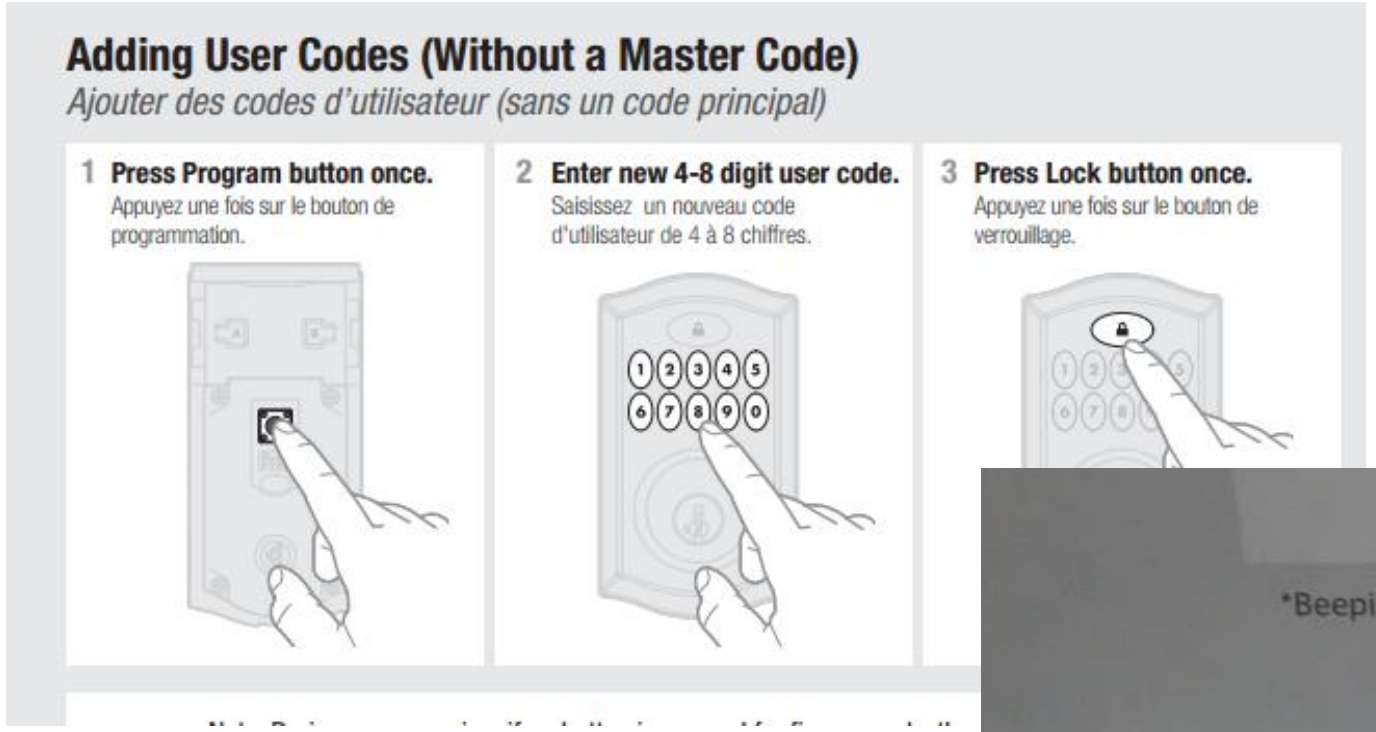


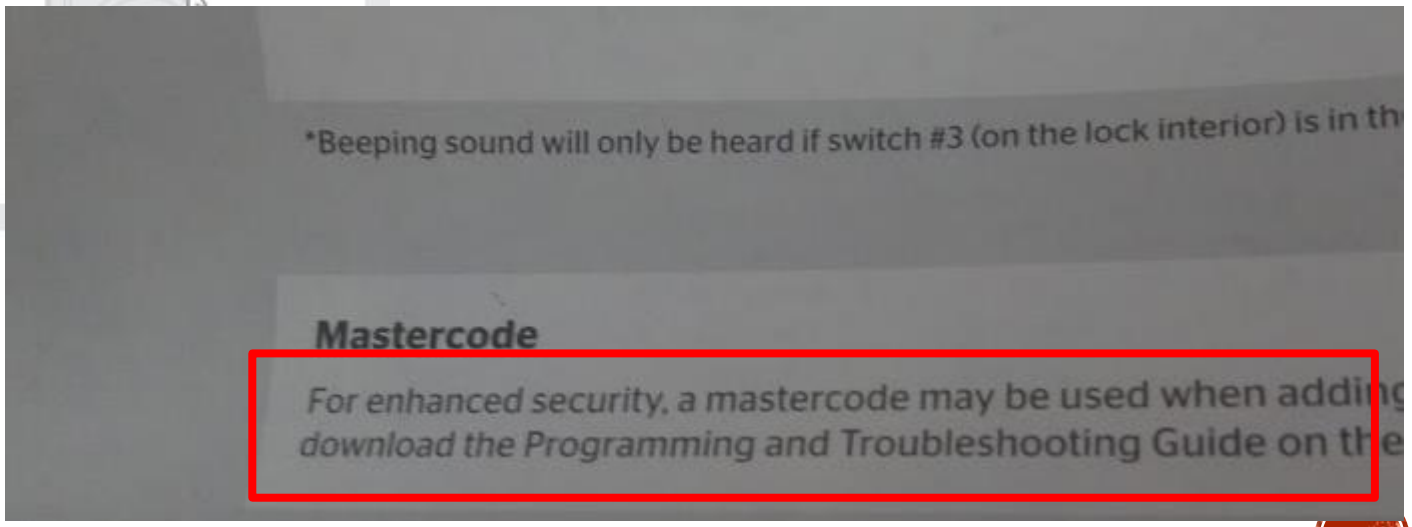
KEYPAD CONNECTION



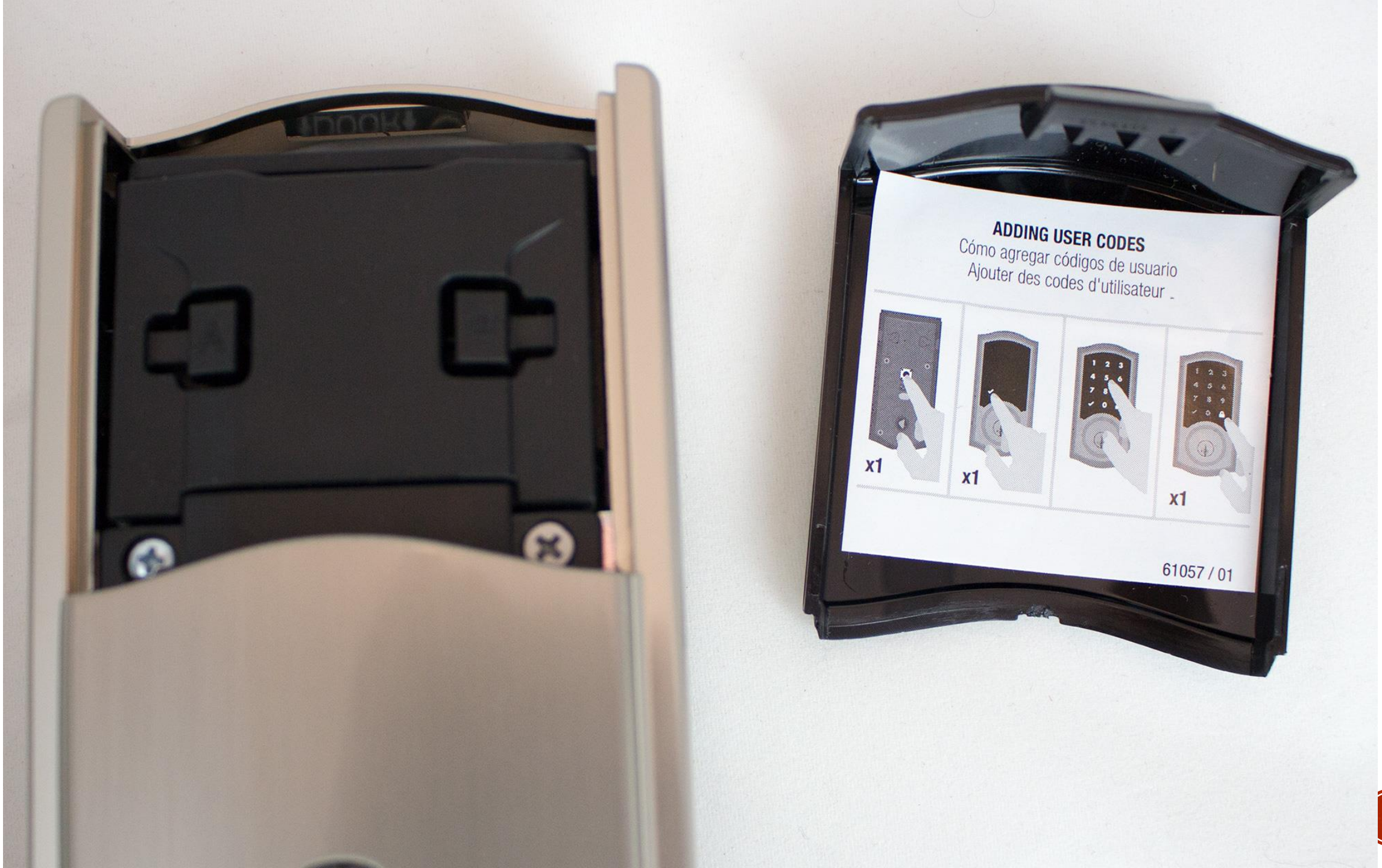
LOCK #2: HOUSE LOCK (VENDOR A)

EVIL MAID ATTACK MADE E-Z



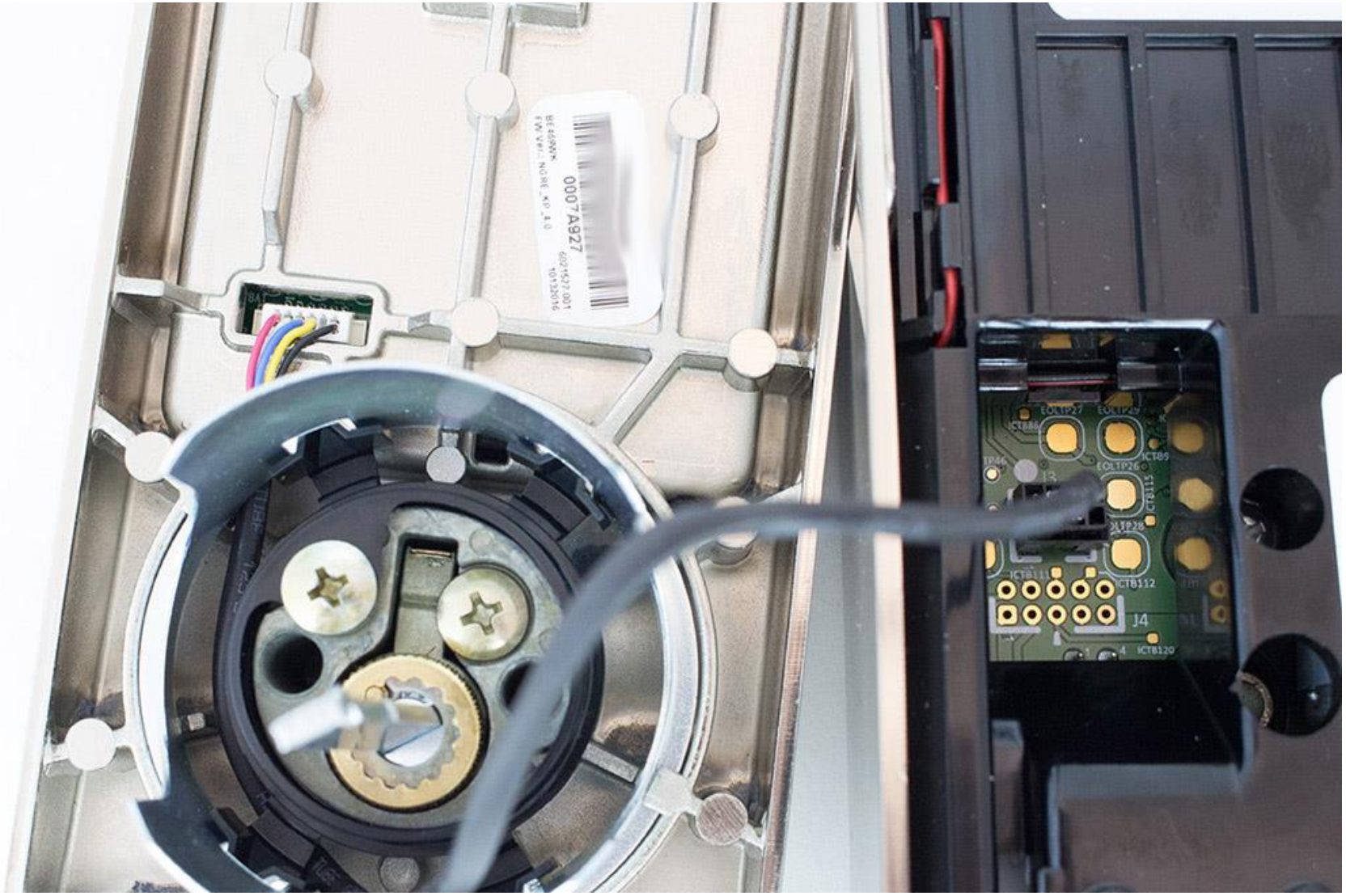


…Don't need special hardware, unless they have gone out of their way you just need access to back of lock for 30 seconds.

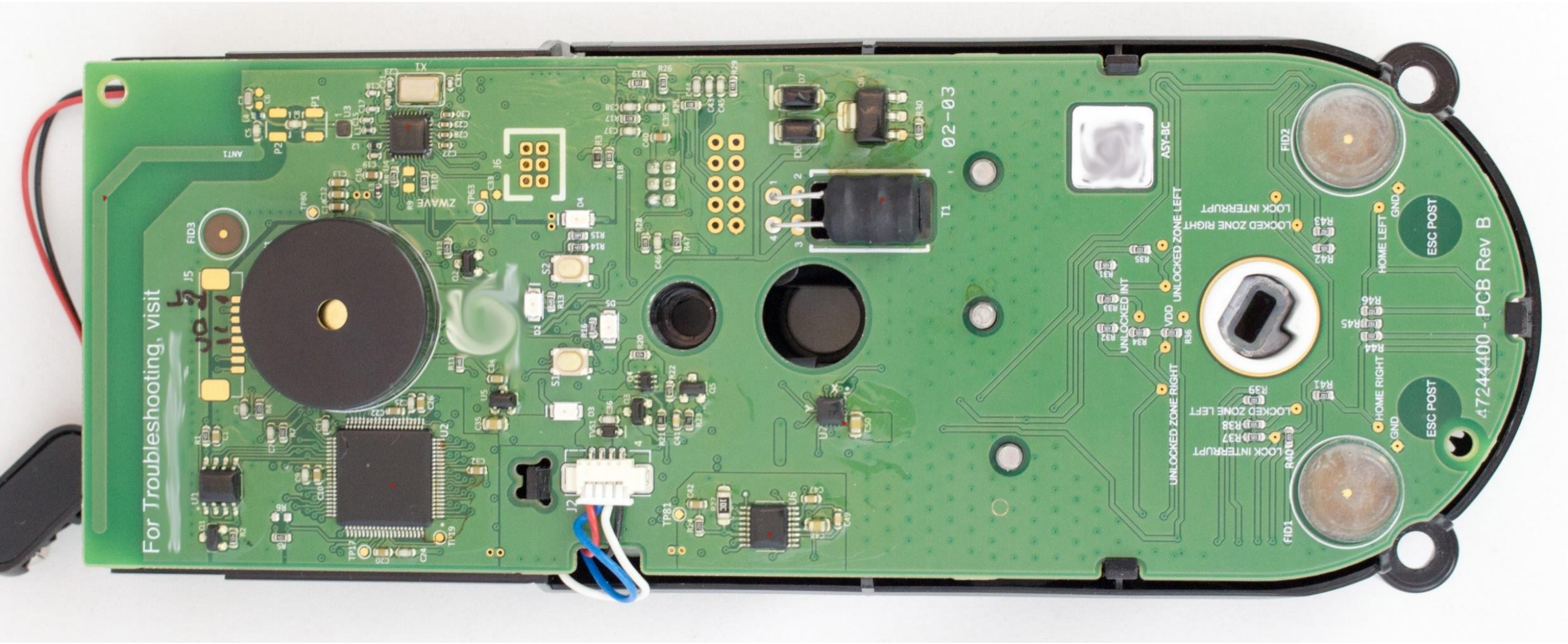

ADDING USER CODES
Cómo agregar códigos de usuario
Ajouter des codes d'utilisateur
x1
x1
x1
61057 / 01

LOCK #3: HOUSE LOCK (VENDOR B)

KEYPAD TO BACKEND CONNECTION



PCB Antenna ZW0301 – Zwave Radio + Microcontroller (SoC) Transformer to make very loud siren



PIC18F87K22 Microcontroller DRV8833 – Motor Driver LIS3DH (Or similar) – Accelerometer

(Device markings not fully documented)

BACKSIDE

(Test pin headers + black markings added by me)

Z-WAVE CONNECTED?

- I haven't looked at Z-Wave side yet

- Lots of good research about Z-Wave security, see for example:
  - https://www.sans.org/reading-room/whitepapers/internet/security-assessment-z-wave-devices-replay-attack-vulnerability-37242

ADDITIONAL FEATURES

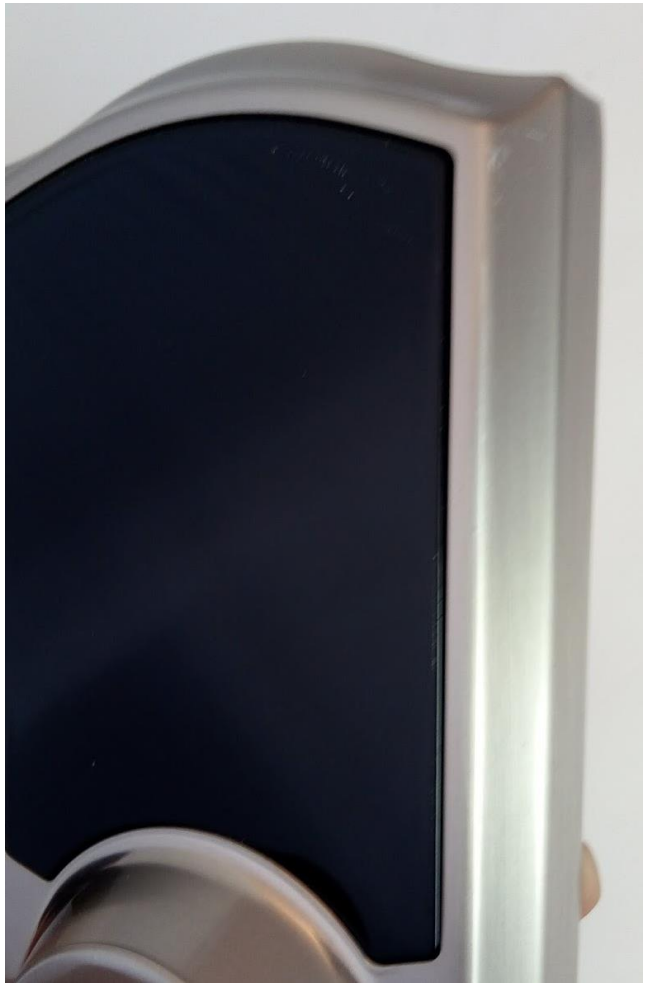
- Accelerometer can detect various levels of tampering depending on adjustable sensitivity:
  - Someone playing with lock when locked (highest level).
  - Someone attempting to force door (medium level?).
  - Someone kicking door down (lowest level).

- Very loud alarm can be enabled when:
  - Physical tampering detected.
  - Too many wrong attempts.

..FRONT PANEL

OOPS?

FOR COMPARISON: VENDOR A FRONT PANEL



WHAT'S ON THAT CABLE?

+VBAT (From 4x AA Cells)
+3.3V (for logic)
Serial RX/TX

SPOOFING FRONT PANEL?

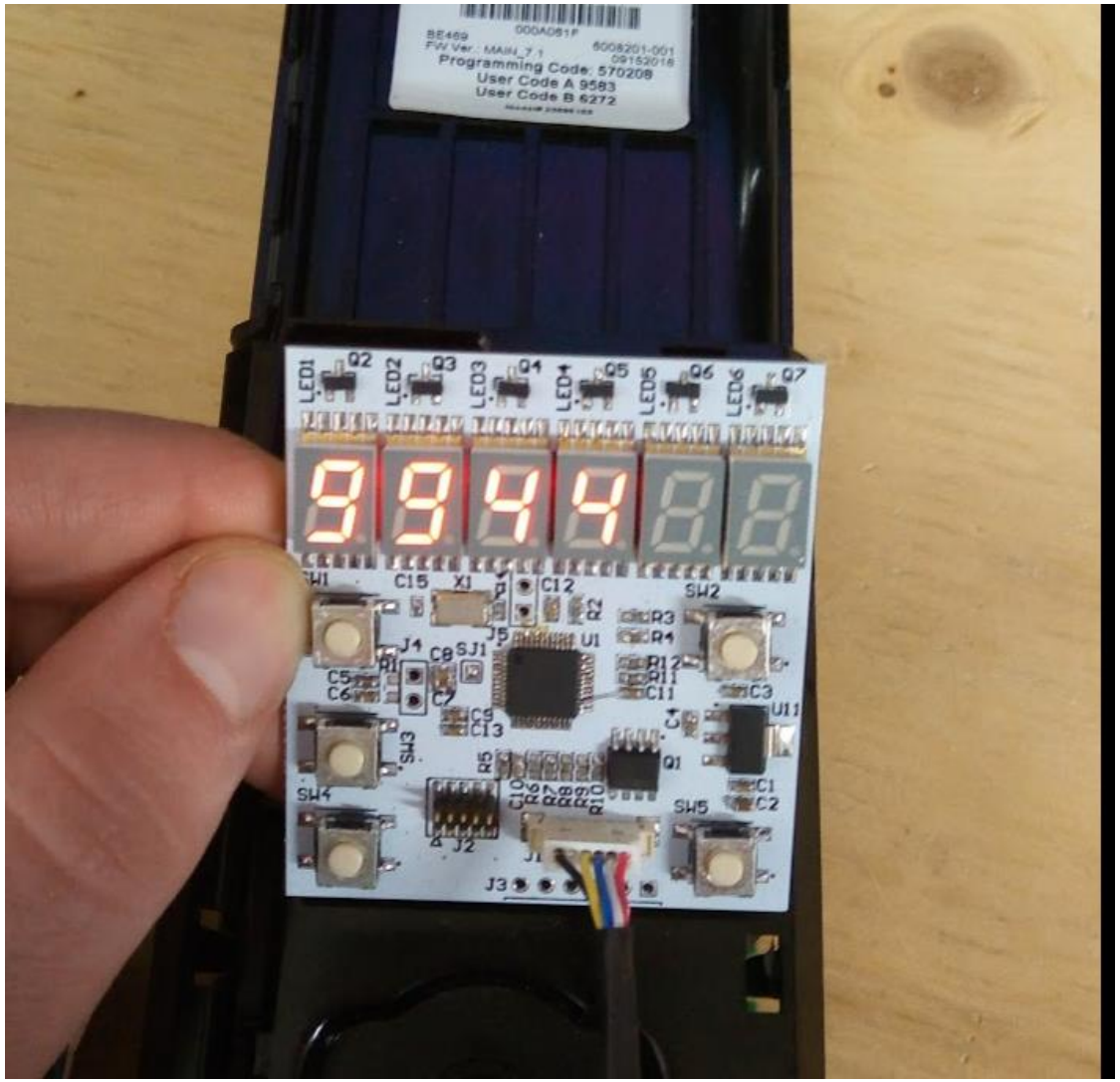
- Simple serial protocol (19200 baud), sends button-press to backend.
- Backend sends messages to turn on lights (green/red) indicating status.
- How fast of messages can you send?
  - Way too fast…

```
void send_cmd(uint8_t * cmd);
void send_guess(unsigned int * guess, unsigned int guess_len);

void send_cmd(uint8_t * cmd)
{
    for (unsigned int i = 0; i < CMD_LEN; i++){
        usart_serial_putchar(CONF_UART, cmd[i]);
    }
}

void send_guess(unsigned int * guess, unsigned int guess_len)
{
    for (unsigned int i = 0; i < guess_len; i++){
        send_cmd(num_buts[guess[i]]);

        //No delay needed!
        //delay_ms(100);
    }
}
```

BYPASSING TIME-OUT, ALARM

1. Power is routed to front panel.
2. Microcontroller needs power to operate.
3. We can short out power to microcontroller to “reset” it, or to disable the alarm.

BREAKING LOCKS... LIKE THE MOVIES!



DEMO – LOCK "HACKING" LIKE THE MOVIES

ABOUT THE ATTACK MODULE

- A little over 120 tries/min
- Searches 4-digit key space in ~85 min
- Tries 3 or 4 PINs, then uses electronic switch to short out power causing lock to reset.
  - Trying 4 pins faster, but may trigger alarm causing short "chirp" before lock resets.
  - Trying 3 pins is stealthy (shown here).

BONUS – FINDING PROGRAMMING CODES

- Programming is a 6-digit code (by default), user codes are 4-digit.
- Brute-force algorithm:
  - Send 4 digits
  - Check response – is it an "error" or "ok"
- If NO response – lock is waiting on more digits.
  - Know first 4 digits of programming code now, need to brute force remaining.
  - Additional ~1 min

FIXES – BRUTE FORCE PREVENTION

- Add power-up delay (shout-out to suggestion by Julien Savoie)
  - Nobody would care if lock takes 30 seconds after putting batteries in to work.
- Enforce reasonable button delay.
- Short timeout after each wrong guess.
- Store timeout to internal memory
  - MUST write this value to memory BEFORE doing the comparison…

FIXES – ALARM DISABLE (ALSO HELPS WITH BRUTE FORCE)

- Add circuit in VCC line (and VBAT if it's needed).
  - Possible to fix with simple physical new cable mailed out:

- Maybe also add resistor to current-limit power to front-panel (such not possible to short out backend)

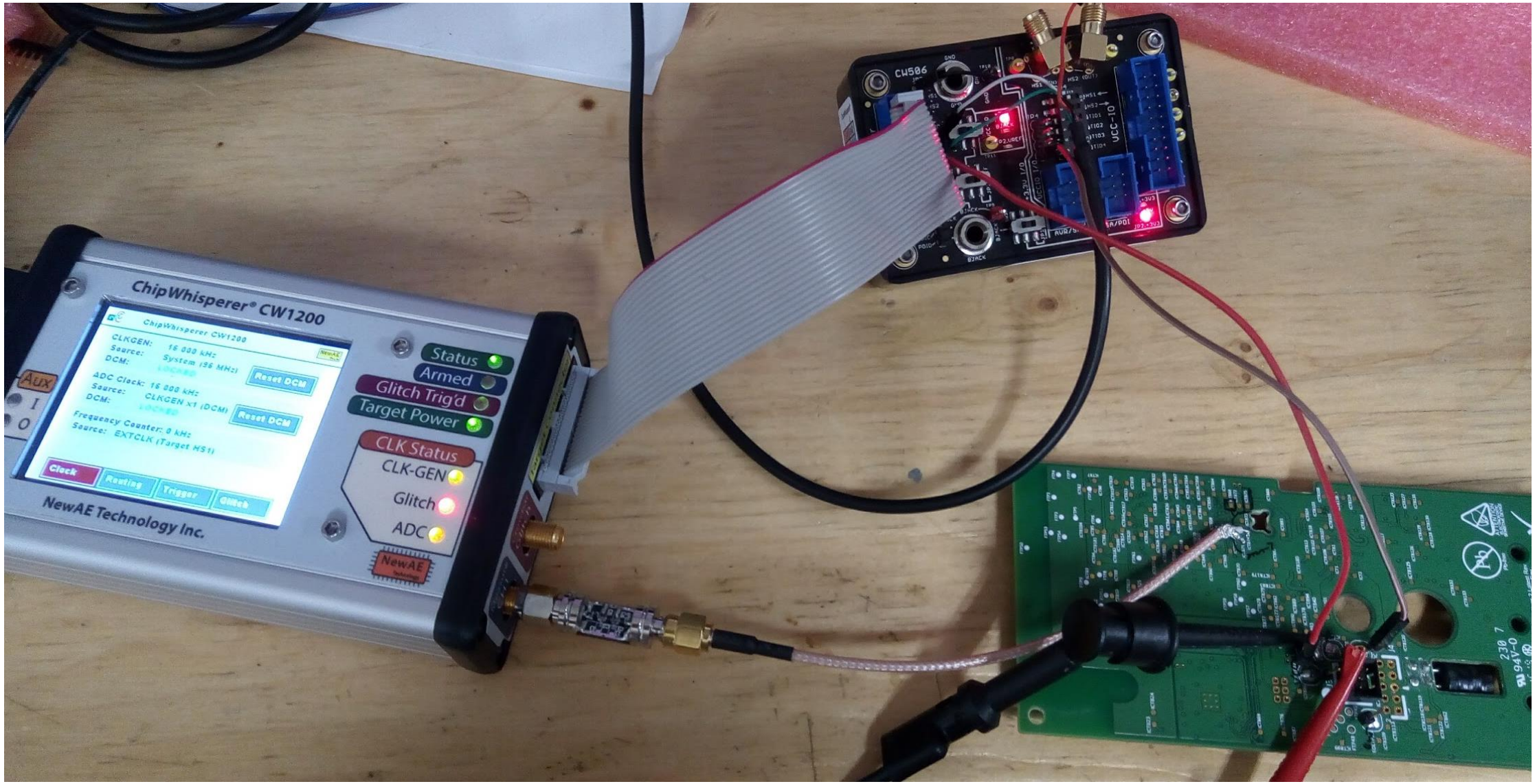
OPEN ISSUES

- Haven't tried fuzzing serial interface.
- Haven't even *looked* at Z-Wave side.
- Possible to perform glitch attacks as have easy access to VCC line.
- Power analysis of the lock also may be possible…

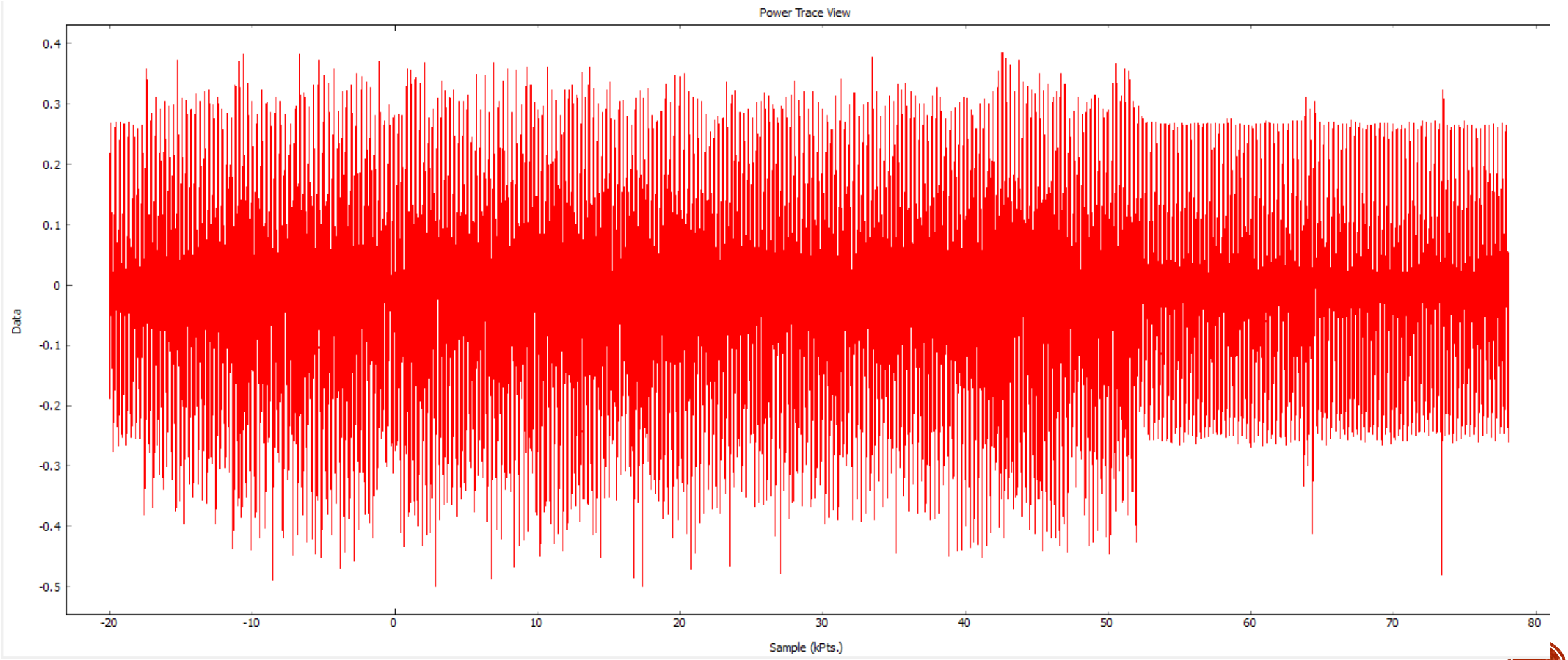
POWER ANALYSIS?

Appears power spikes measurable at front keypad… Also opens up power analysis.
Following slides show preliminary stages of this work (measuring at backend instead):

POWER ANALYSIS (PRELIMINARY)



POWER ANALYSIS (PRELIMINARY)



NOTE ON VENDOR RESPONSE TO THIS

- Vendor was notified – they have been *extremely receptive* and are working on a fix, along with some general improvements beyond the one particular flaw (I have redacted full details for now on account of that).

MORE?

Blog	OFLYNN.COM
Company	NEWAE.COM
Twitter	@colinoflynn