Security alarm system — feeling of security or cause for alarm?

Kirils Solovjovs
https://kirils.org/

Author

- Lead researcher at Possible Security, Latvia
- Hacking and breaking things
  - Network flow analysis
  - Reverse engineering
  - Social engineering
  - Legal dimension
- Follow me on twitter / @KirilsSolovjovs

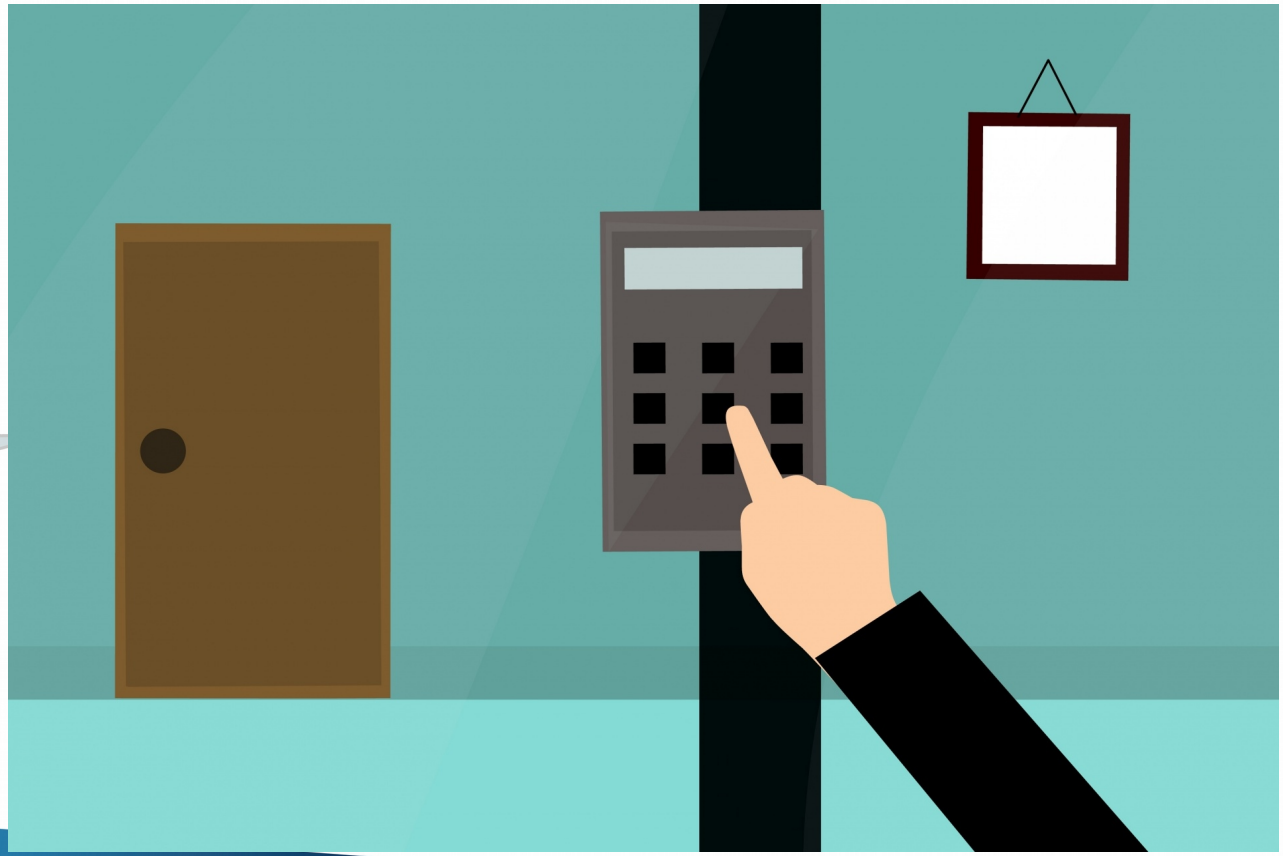
NULLCON
INTERNATIONAL SECURITY CONFERENCE

What's new?

- Alarm systems
- Paradox intro
- Radio specs for remote ✓
- Attack tool development ✓
  - M5Stack ✓
- First steps in firmware reverse engineering ✓

Skip to page 14 if you've seen previous presentations

Security alarm systems

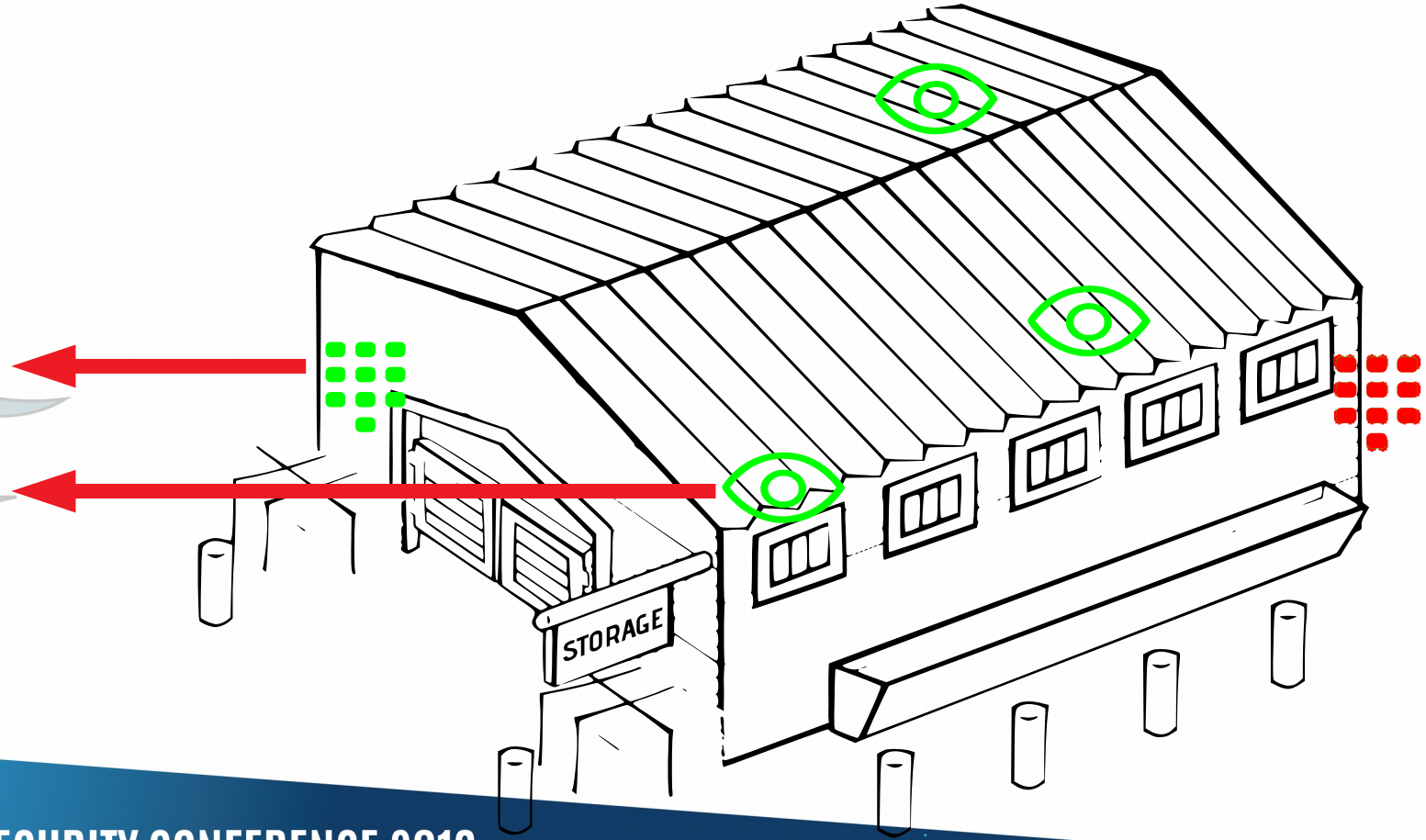


Security alarm systems

What could go wrong?

```
3998 3111 9309 1400 8248
4584 9450 5617 6550 8245
6979 9878 6101 4971 1294
9576 5005 2789 3013 3627
6856 5132 4920 5076 7500
7065 0643 9302 1744 3725
8432 1275 1128 1497 8657
9264
```

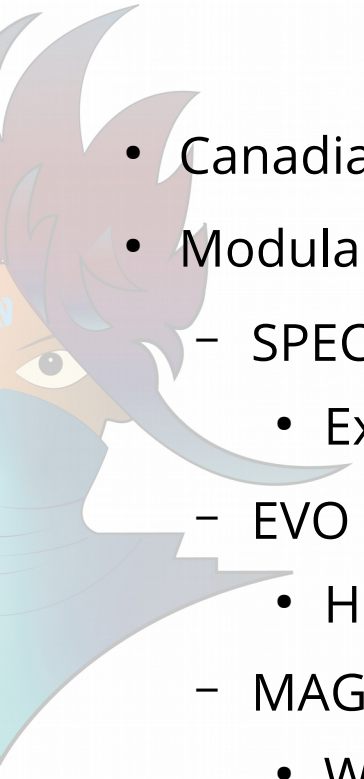
Does this provide a feeling of security?



NULLCON
INTERNATIONAL SECURITY CONFERENCE

INTRO

Paradox security systems

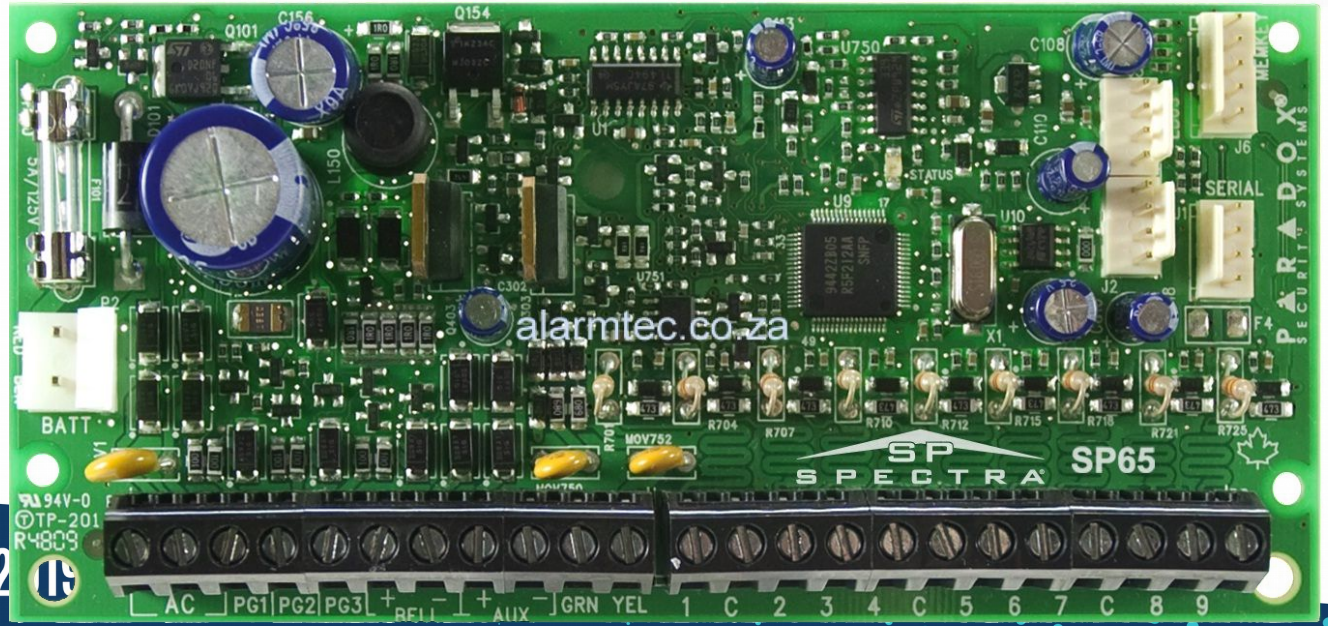


- Canadian company, founded 1989
- Modular security alarms
  - SPECTRA SP
    - Expandable Security Systems
  - EVO
    - High-Security & Access Systems
  - MAGELLAN
    - Wireless Security Systems

Main components

- **master**

  heart on the system – “motherboard”
  - panel
- **ancillaries**
  - battery
  - power supply
  - siren

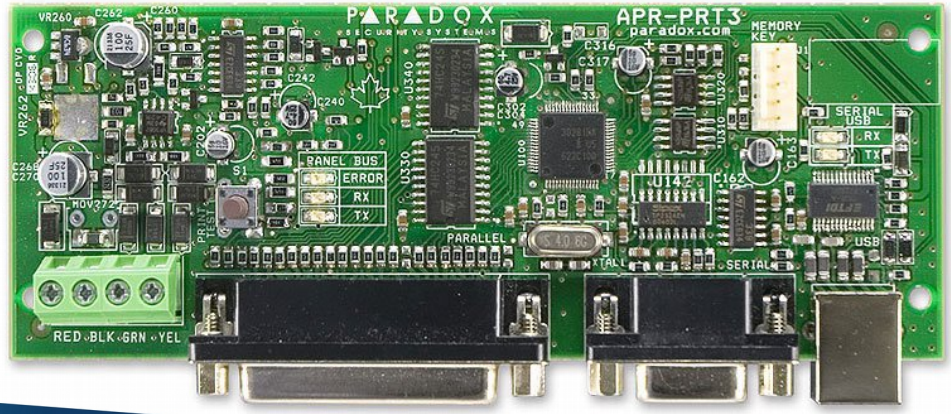


Main components

- **combus slaves**

  provide two-way communication

  - keypads
  - modules
    - expansion
    - printer
    - listen-in
    - etc.

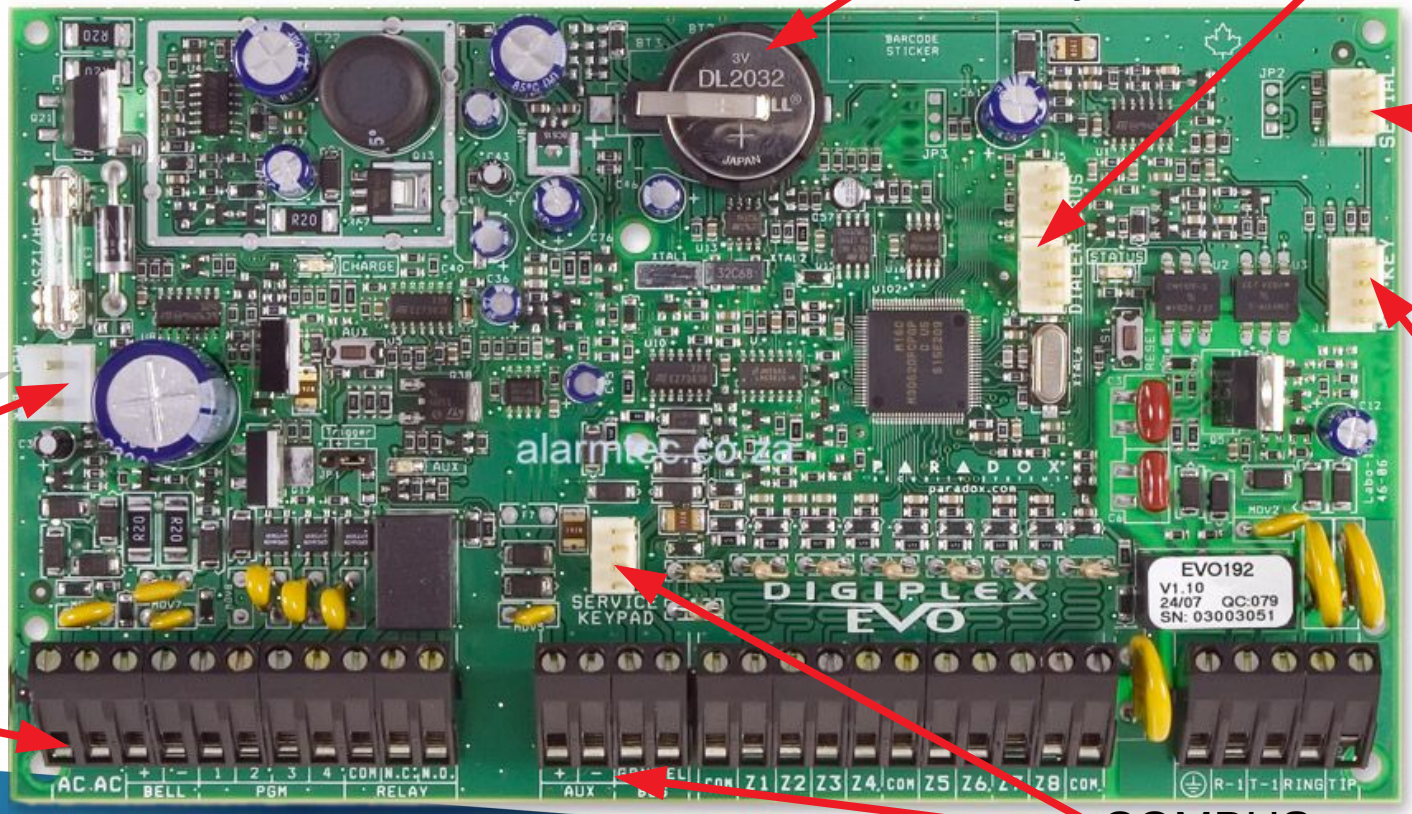


Main components

- **zone** interrupt devices

  input, measures resistance ⇒ chaining
  - magnetic sensors
  - PIR sensors
  - panic buttons
  - etc.

EVO192



NULLCON
INTERNATIONAL SECURITY CONFERENCE

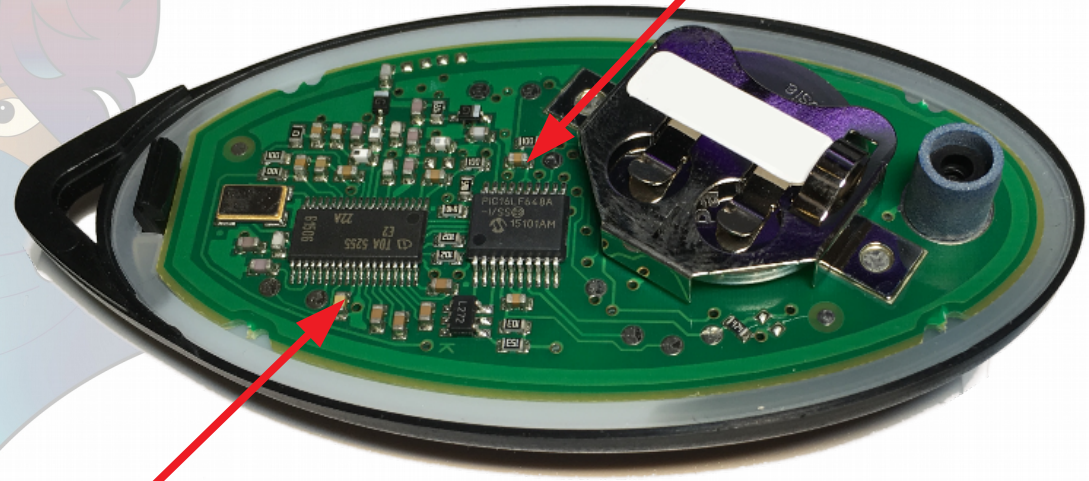
NULLCON
INTERNATIONAL SECURITY CONFERENCE

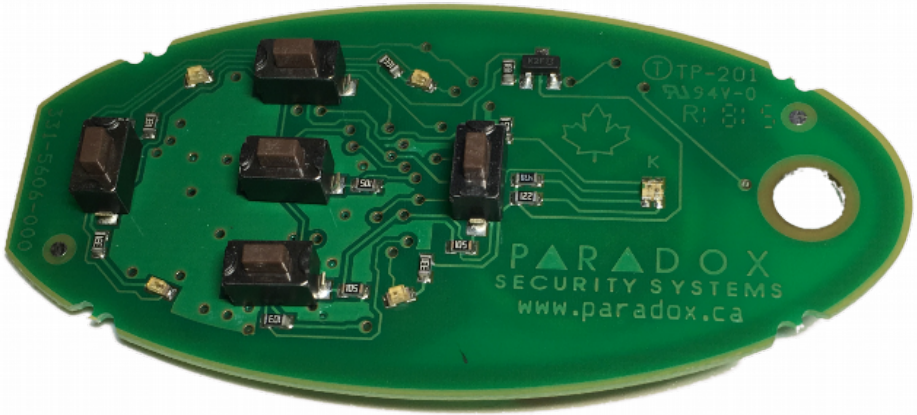
RADIO

Remote REM2

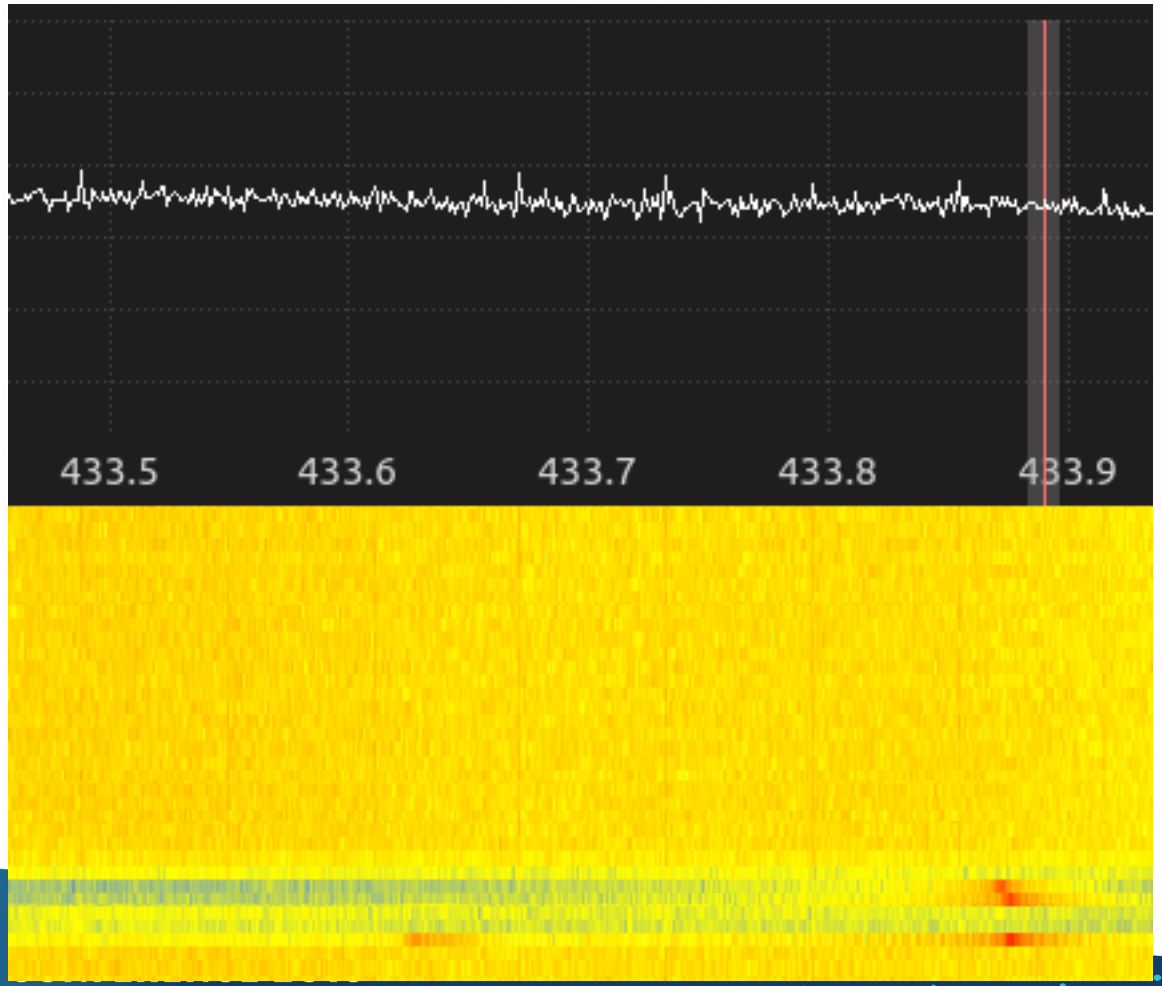
- Two-way comms!

Opening it up



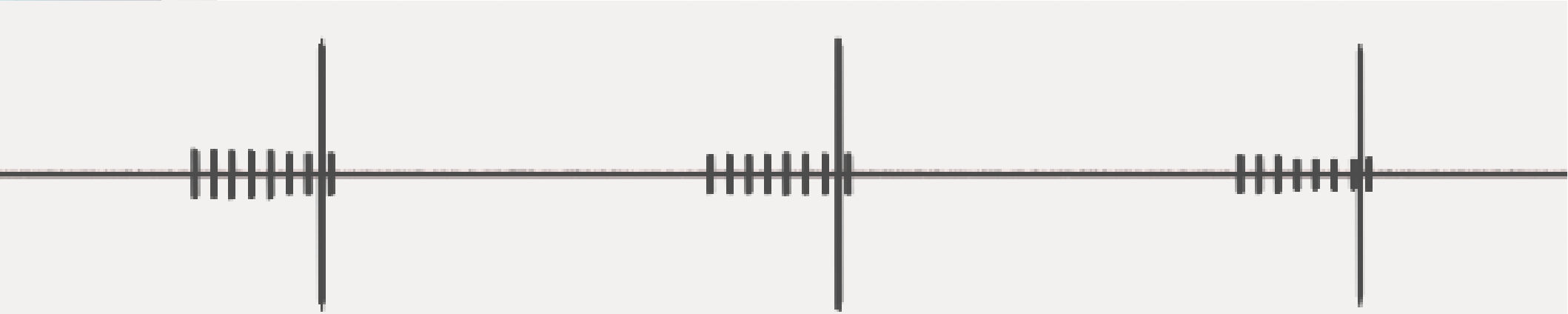


There it is



We gotta go closer

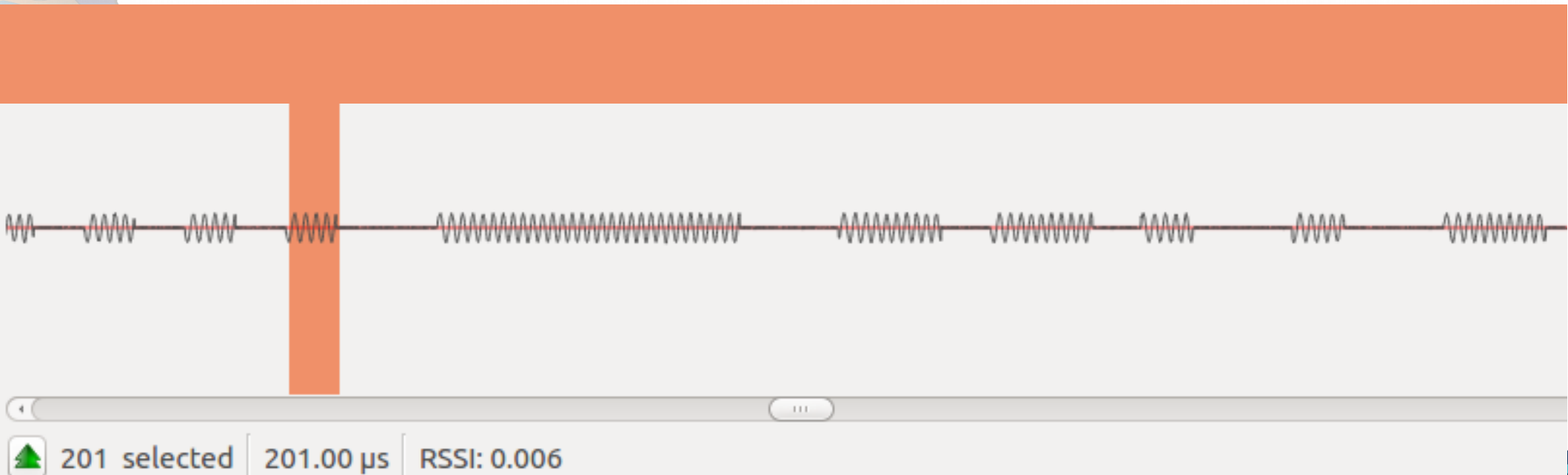
- ~ 433.9MHz, Tx and Rx share the same channel
  - same packet sent in short bursts (8 times)
  - 1 reply from panel




LOOK CLOSELIER
LOOK MORE CLOSELIER
quickmeme.com

... closelier

- 1-level ASK
- bit length = 200µs



Structure

- init = 1111
- synchronization preamble = 01010101010101010101010101
- packet length – init (4b) + preamble (24b) + data (112b)
- to be continued elsewhere :-)

NULLCON
INTERNATIONAL SECURITY CONFERENCE

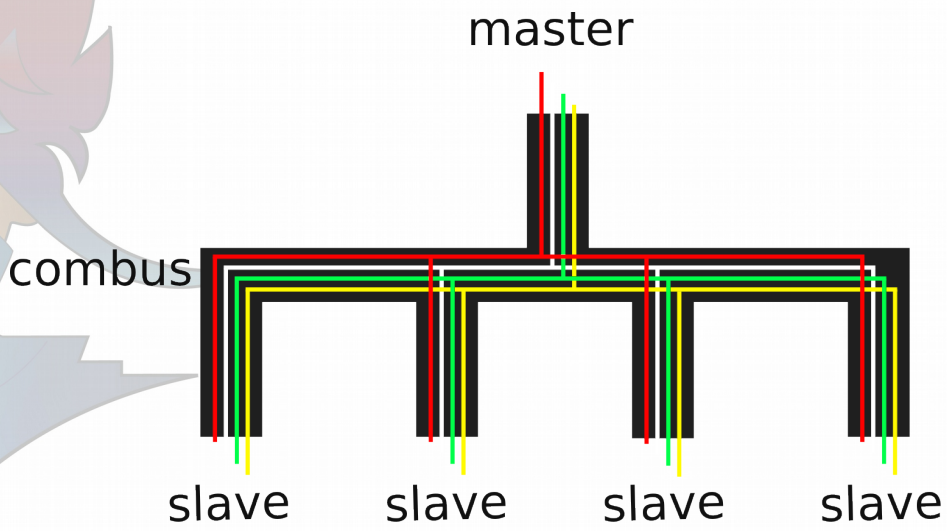
ATTACK TOOL

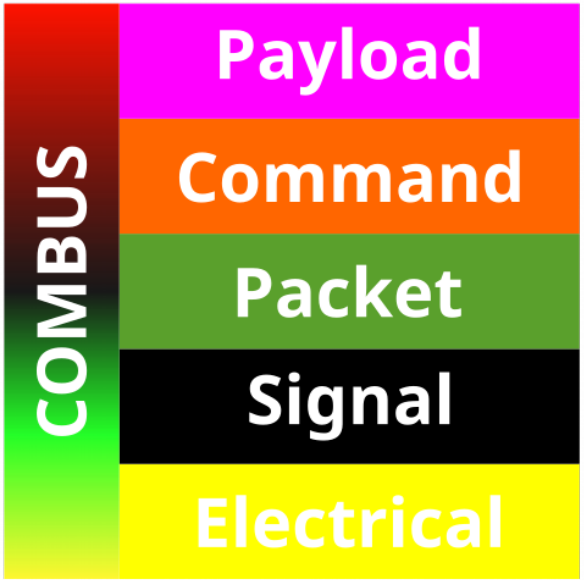
M5Stack


M5
CORE
GND ADC G35
GND ADC G36
GND RST EN
G23 MOSI DAC/SPI G25
G19 MISO DAC G26
G18 SCK 3.3V
G3 RXD0 TXD0 G1
G16 RXD2 TXD2 G17
G21 SDA SCL G22
G2 GPIO GPIO G5
G12 IIS_SK IIS_WS G13
G15 IISOUT IIS_MK G0
HPWR IIS_IN G34
HPWR 5V
HPWR BATTERY
ESP32
2018.3

M5Stack

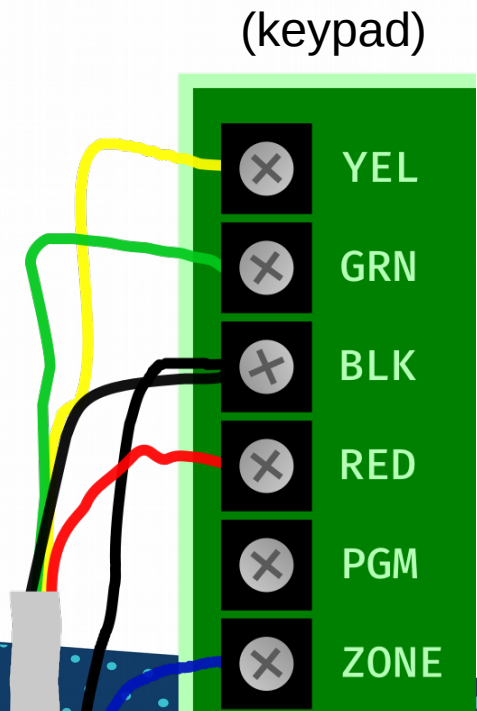
COMBUS


master
combus
slave
slave
slave
slave


COMBUS
Payload
Command
Packet
Signal
Electrical

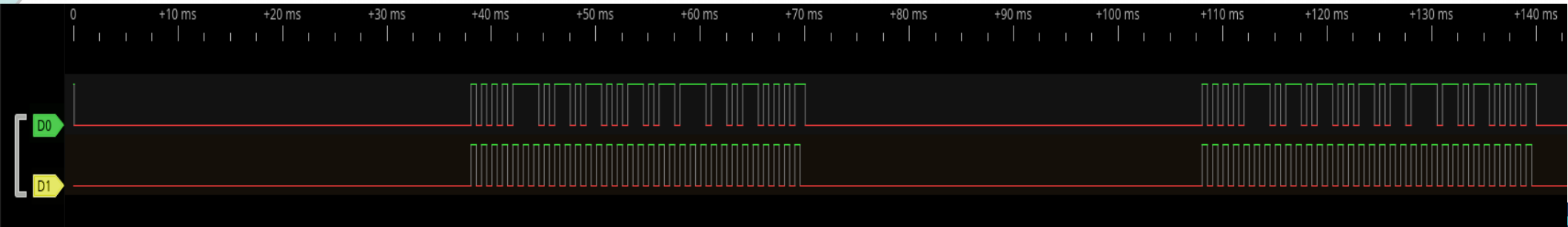
Electrical layer

- combus – 4 wire bus
  - black = GROUND
  - red = POWER
  - yellow = CLOCK
  - green = DATA



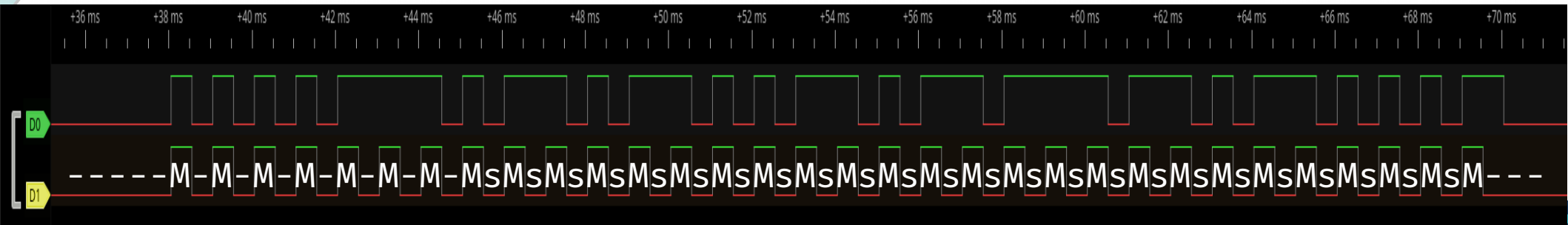
Signal layer

- 40ms between packet bursts
- 1 clock cycle = 1ms; signal = 1kHz

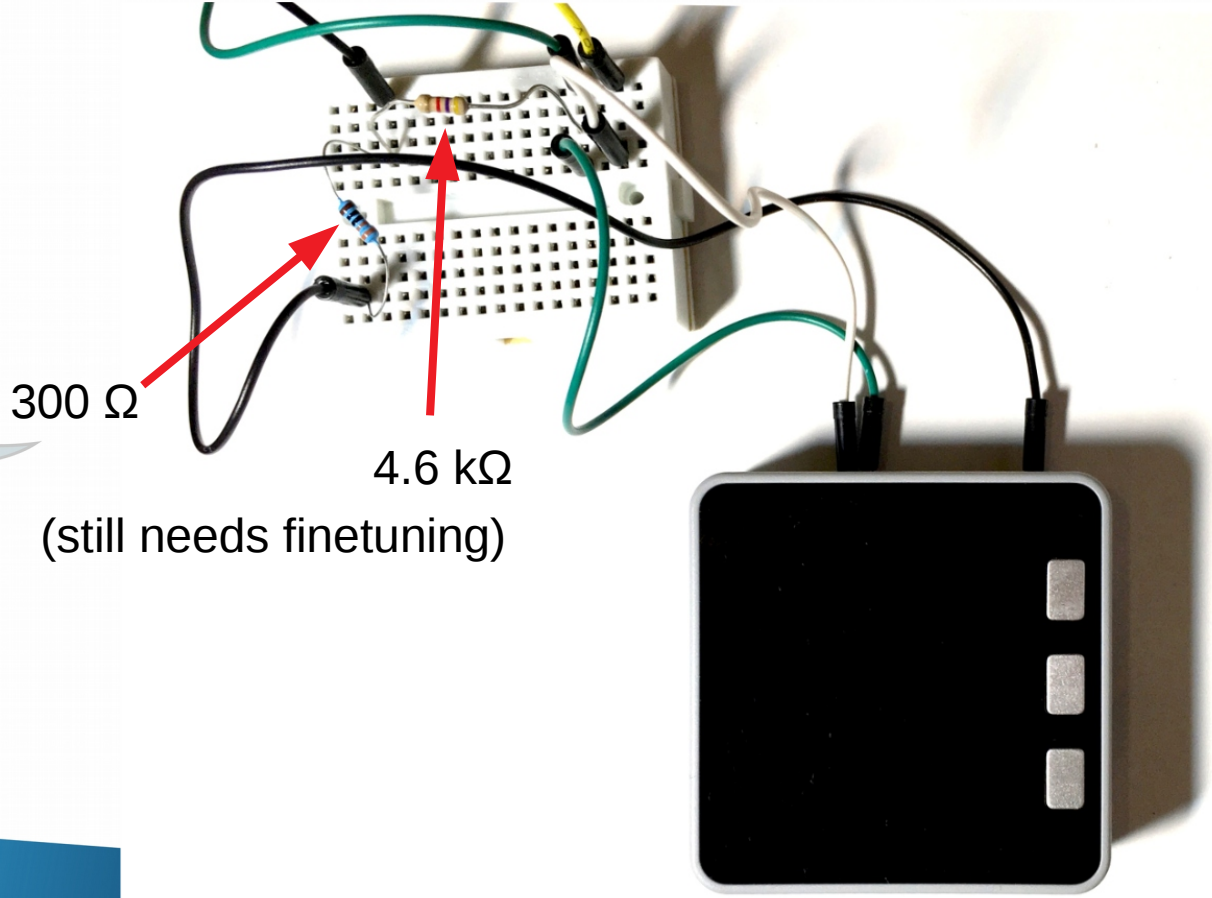


Full signal encoding

- CLOCK = high
  - slave pulls down to send “1”
- CLOCK = low
  - master pulls up to send “1”



Hardware setup



Packet structure

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
master																						
E2	14	10	0B	0F	37	05	00	01	5D	~~00~~												
0C	13	38	1B																			
slave																						
~~00~~	02	00	00																			
~~00~~	02	20	00	00	00	FF	5A	22	00	00	00	00	D5	23	79	E2	00	00	00	C8	B6	00

command | checksum | ~~unused~~ | channel-request

Checksum

```
checksum ← 0
for i in @command to @checksum - 1:
  checksum ← (checksum + *i) % 100
```

Payloads

- No encryption used
- Text as fixed length (often 16

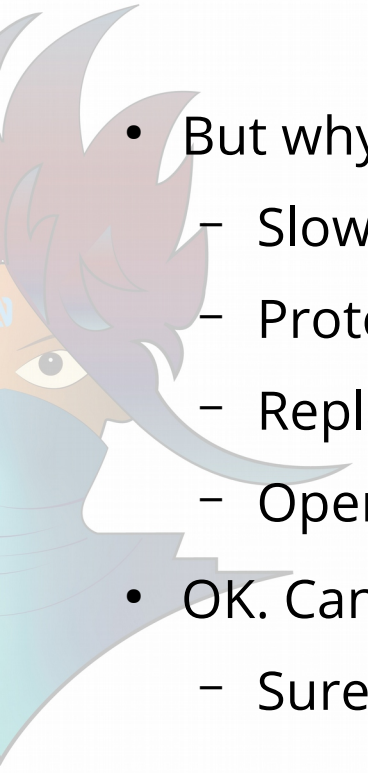
```
b0 02 00 00 00 44 6f 6f | .....Doo
72 20 30 31 20 20 20 20 | r 01
20 20 20 20 20 e7 00    |       ..
```

  - 0x20 = filler
- Numbers usually packed BCD
  - “0” is 0b1010 = 0xA
  - no encryption, but hey, at least we got obfuscation!

NULLCON
INTERNATIONAL SECURITY CONFERENCE

DEMO ONE

Spoofing data / keypad emulation



- But why?
  - Slowly bruteforcing stuff
  - Protocol fuzzing
  - Replay attacks
  - Open source keypads?
- OK. Can we?
  - Sure we can!

NULLCON
INTERNATIONAL SECURITY CONFERENCE

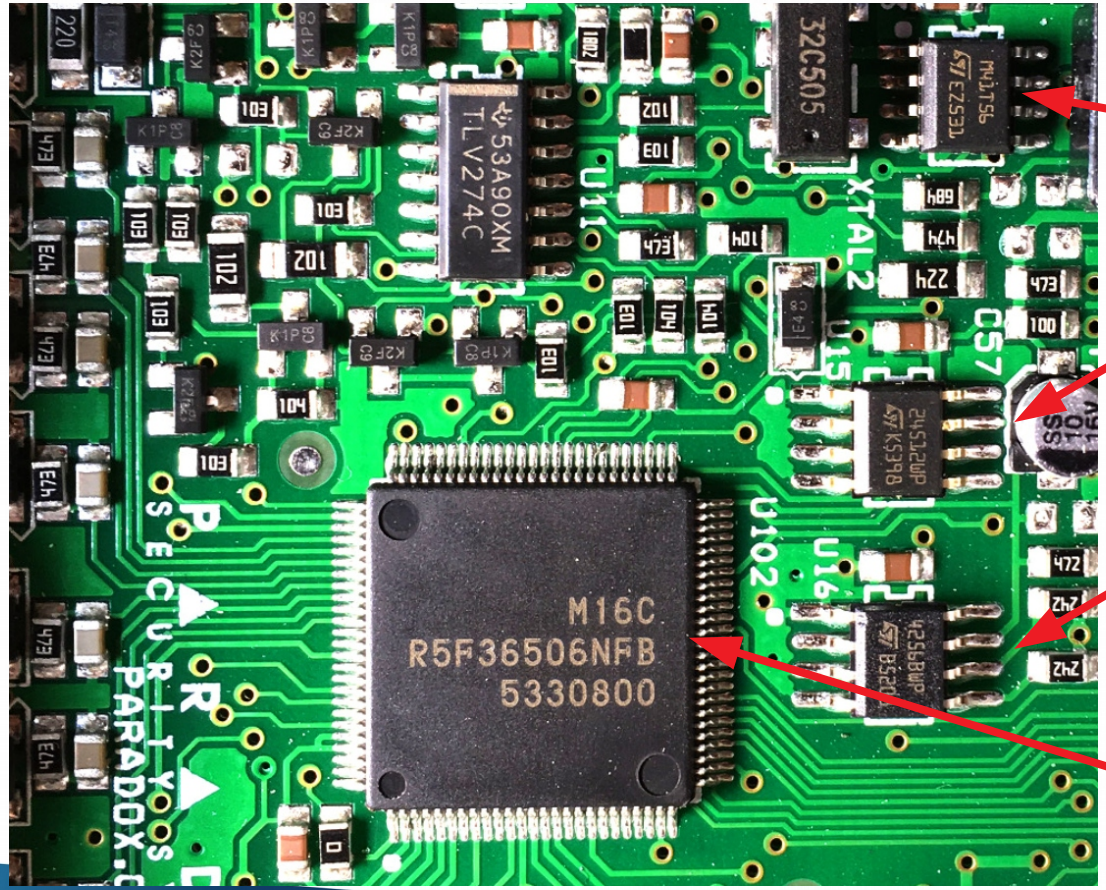
DEMO TWO

NULLCON
INTERNATIONAL SECURITY CONFERENCE

FIRMWARE INTRO

(Look for a conference near you!)

CHIPS



STM M41T56, RTC, 56B NVRAM

STM 24512WP, EERPOM, 64KiB, page=128b

STM 4256BWP, EERPOM, 32KiB, page=64b

RENESAS R5F36506, MCU, ROM 128KiB+16KiB, flash 4KiB, RAM 12KiB

Now what?

+

+ coding missing support

NULLCON
INTERNATIONAL SECURITY CONFERENCE

SUMMARY

EVO192

“Digiplex and Digiplex EVO systems provide the highest level of protection for banks, high-security military and government sites, luxurious residential homes and any place where maximum security is essential.”

– https://www.paradox.com/Products/default.asp?CATID=7

Results

- Attack tool based on M5Stack created
  - active keypad emulation support
- (Some) RF attacks tested
- Firmware reverse engineering unlikely, however EEPROM can be read

Further research

- Make attack tool even more modular & more functional
  - Find the right resistors!
- Continue testing RF attacks
- Pull configuration (including codes) from EEPROM
- COMBUS over radio (MG?)

Links. Q&A?

Slides on https://kirils.org/

Tools on https://github.com/0ki/paradox

I’m on https://twitter.com/KirilsSolovjovs