

Hackcube

beVX, September 2018

We Love Hardware && Not Only Hacking

About @sgniwx and why I am here



The Shepherd Lab

Day Time Job, breaking things and earning salary

- > IoT Research
- > Blockchain Research
- > Fun Security Research



HACKERSBADGE.COM Reverse Engineer Badge Maker

Founder of hackersbadge.com, RE && CTF fan

- > Reversing Binary
- > Reversing IoT Devices
- > Part Time CTF player



Security Conference

Hack in the box, Netherland and Singapore. Soon to be Beijing and Dubai

- > 2006 till end of time
- > Core Crew
- > Review Board

- > 2005, HITB CTF, Malaysia, First Place /w 20+ Intl. Team
- > 2010, Hack In The Box, Malaysia, Speaker
- > 2012, Codegate, Korean, Speaker
- > 2015, VXRL, Hong Kong, Speaker
- > 2015, HITCON Pre Qual, Taiwan, Top 10 /w 4K+ Intl. Team
- > 2016, Codegate PreQual, Korean, Top 5 /w 3K+ Intl. Team
- > 2016, Qcon, Beijing, Speaker
- > 2016, Kcon, Beijing, Speaker
- > 2016, Intl. Antivirus Conference, Tianjin, Speaker
- > 2017, Kcon, Beijing, Trainer
- > 2017, DC852, Hong Kong, Speaker
- > 2018, KCON, Beijing, Trainer
- > 2018, DC010, Beijing, Speaker
- > 2018, Brucon, Brussel, Speaker
- > 2018, Nanosec, Kuala Lumpur, Speaker
- > 2018, HITB, Beijing/Dubai, Speaker
- > 2018, beVX, Hong Kong, Speaker
- > MacOS SMC, Buffer Overflow, suid
- > GDB, PE File Parser Buffer Overflow
- > Metasploit Module, Snort Back Orifice
- > Linux ASLR bypass, Return to EDX

About @WhiteAl0n3



360 独角兽安全团队
360UNICORNTTEAM

- > Hardware Research
- > IOT Research
- > Fun Security Research



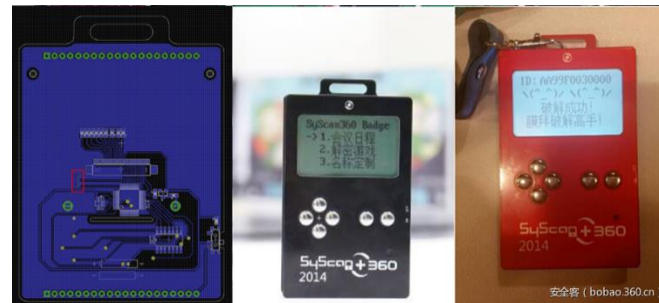
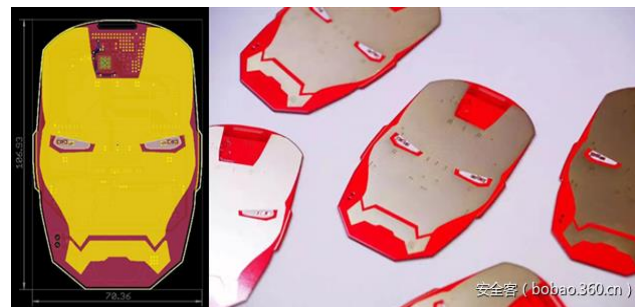
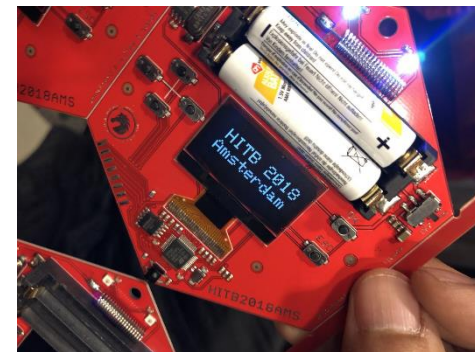
- > Design Hardware
- > Develop MCU
- > Radio Research



HACKERSBADGE.COM

- > Design Badges
- > Develop Code
- > Conference Hopping

- > 2014, co-founder of UnicornTeam
- > 2016, BlackHat USA, Speaker
- > 2016, BlackHat Europe Arsenal, Speaker
- > 2016, ISC, Speaker
- > 2017, founder of RocTeam
- > 2017, BlackHat Asia Arsenal, Speaker
- > 2017, ISC, Speaker
- > 2018, HITB AMS, Speaker
- > 2018, Defcon, Speaker
- > 2018, ISC, Speaker
- > 2013-2017, SyScan360 Badge
- > 2017-2018, DC010 Badge
- > 2018, HITB Badge
- > HackID、HackID Plus
- > HackKEY
- > HackNFC
- > HackPKE
- > HackCUBE



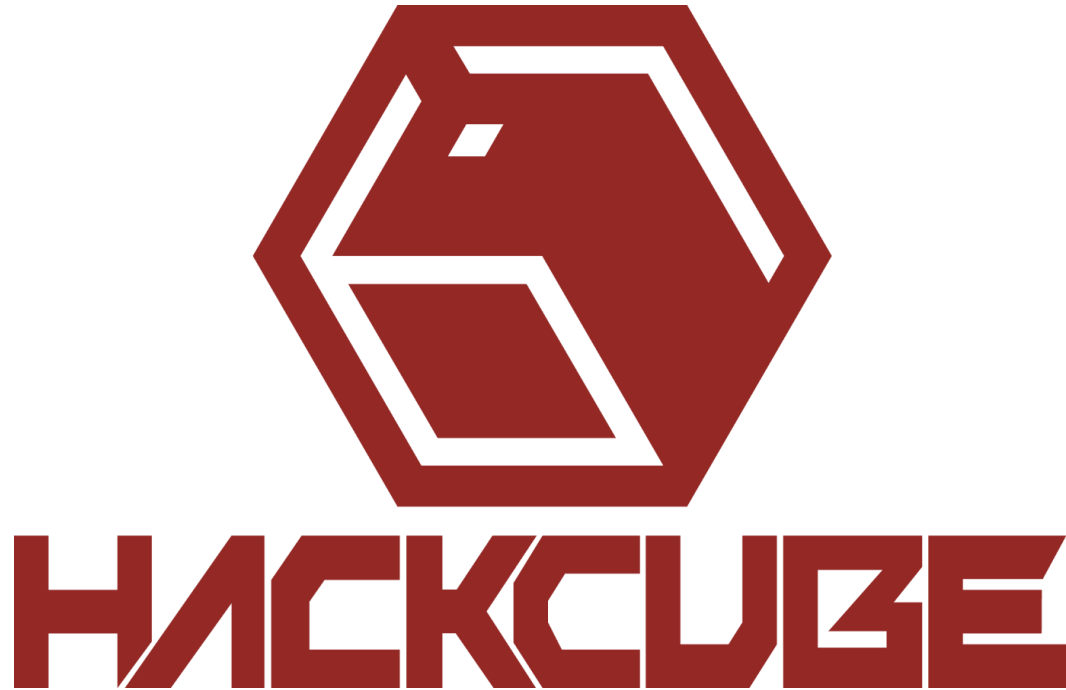
If You Ever Wanted to Start Wireless Hacking

The Development Board and etc



Imagine, during coffee session and decided to start some “research”

What Our Plan



Pandora Box / MacGyver Tools

- ❖ A Leaning Tool, even to students
- ❖ Pentest Kit
- ❖ Its good looking. Not to scare others
- ❖ Interchangeable module
- ❖ Things might not need for now
 - ❖ Maybe a 4G/4G+/5G WiFi Router
- ❖ Or maybe a touch screen or e-ink screen
- ❖ A REAL WIRELESS CUBE *REAL*

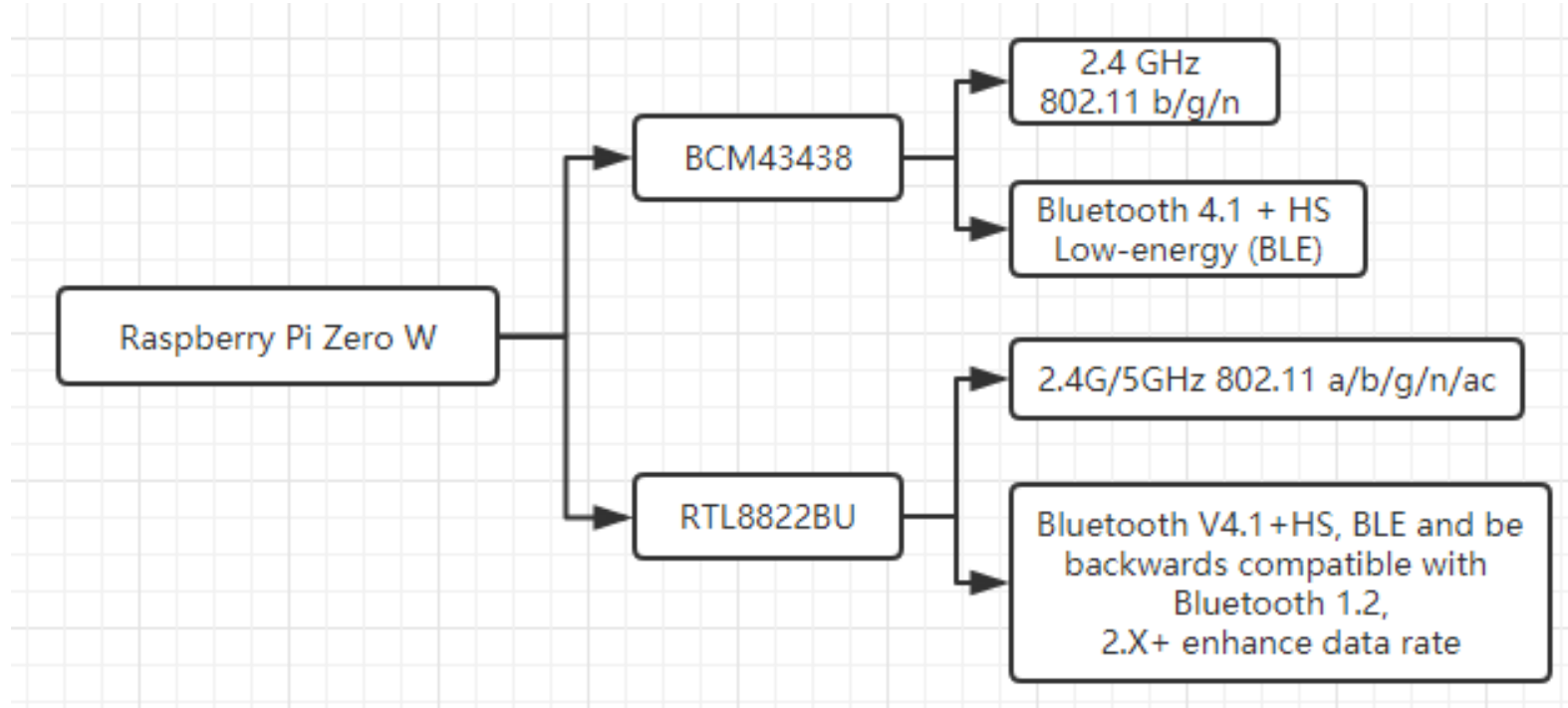
The Game Plan

We Want a Toy, A Really Cool Toy

Fully Open Souce, PCB Design and Code.

Drawing Board

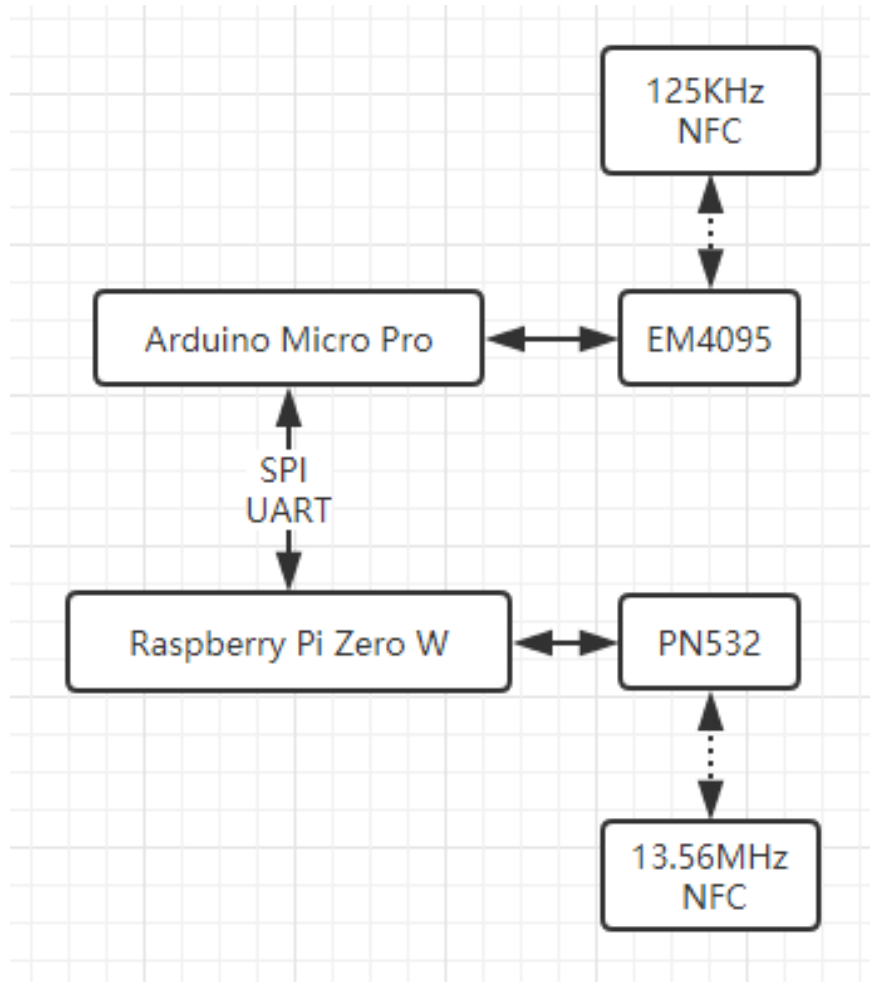
The RF Kit



- ❖ WiFi Router
- ❖ WiFi Advertising
- ❖ WiFi Blocking Attack
- ❖ WiFi Everything

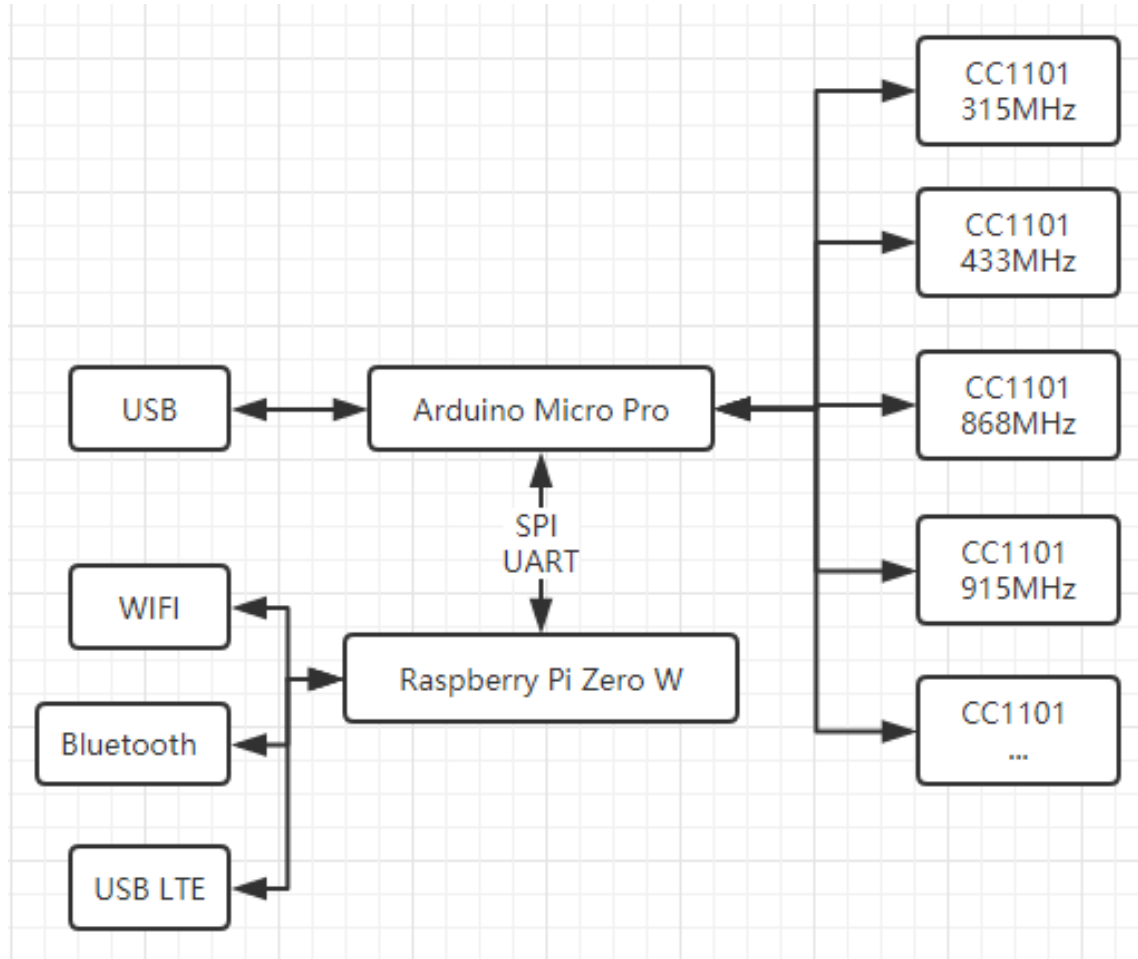
- ❖ Bluetooth Advertising
- ❖ Bluetooth Keyboard/Mouse
- ❖ Bluetooth IoT Gateway
- ❖ Bluetooth Everything

The NFC Kit



- ❖ IoT Sub-1GHz RF Board
- ❖ RFCat
- ❖ HID Attack Tool
- ❖ Remote Control Tool
- ❖ Wireless Keyboard
- ❖ RF Transmit Mode

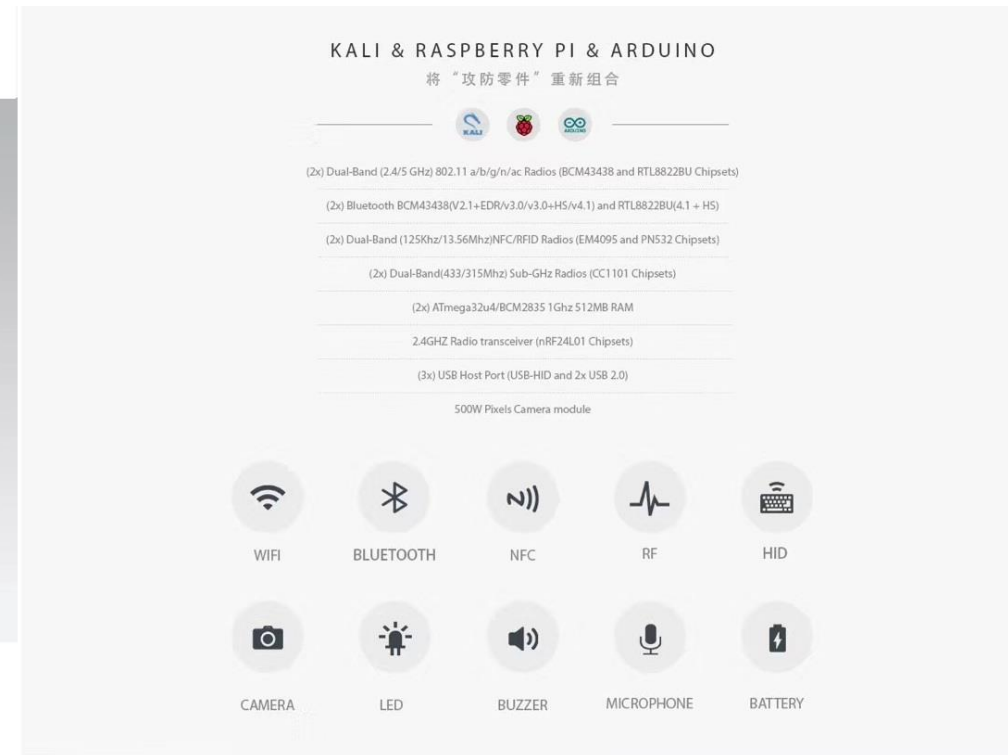
The HID Kit



- ❖ Keyboard
- ❖ USB Network Card
- ❖ USB Disk
- ❖ BadUSB

The BETA

The CUBE, The BETA

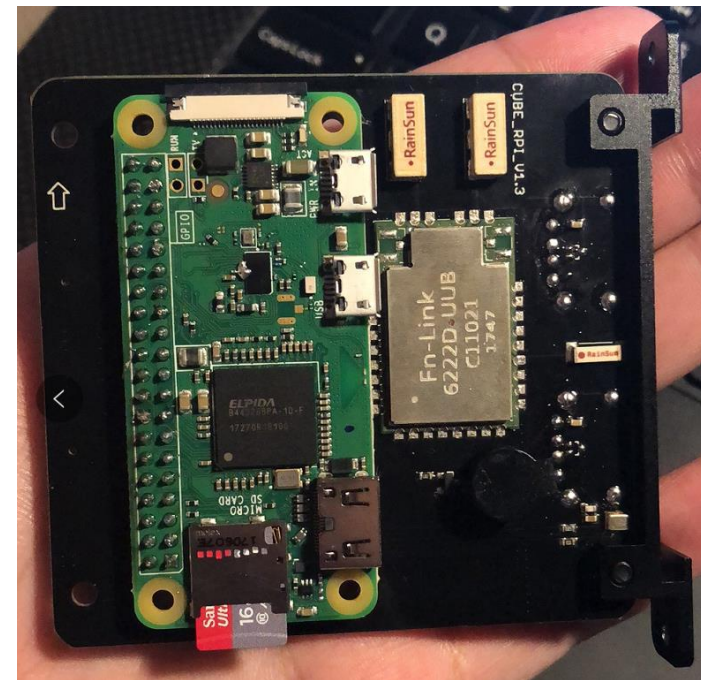
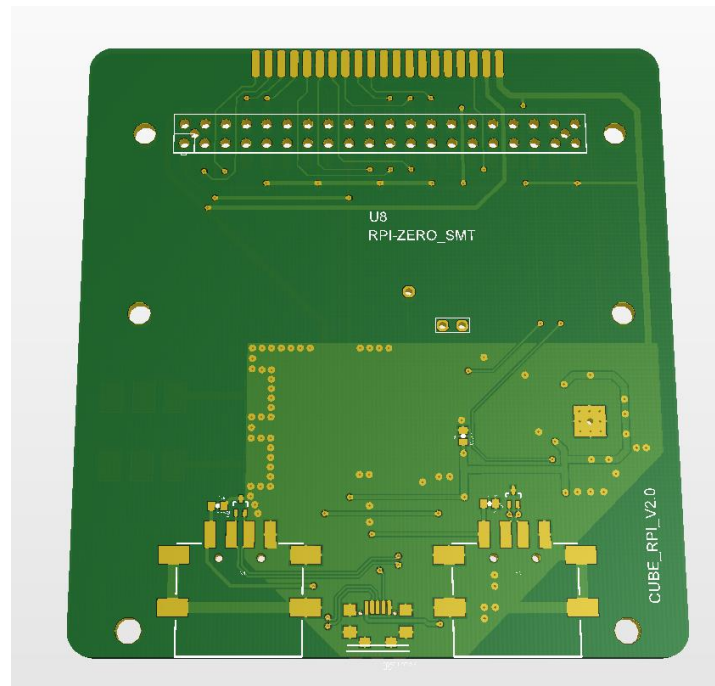
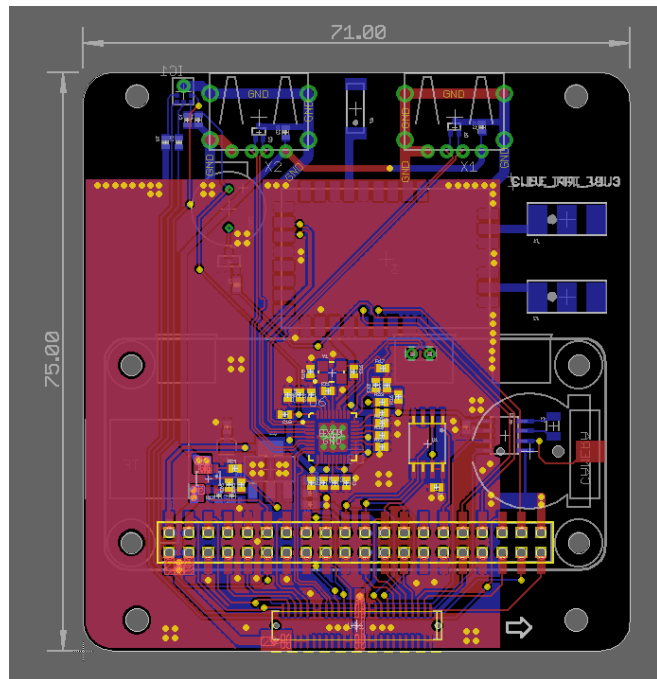


HackCUBE with all possibilities

Working On a Better Version

Not as easy as “git push”

Main Board



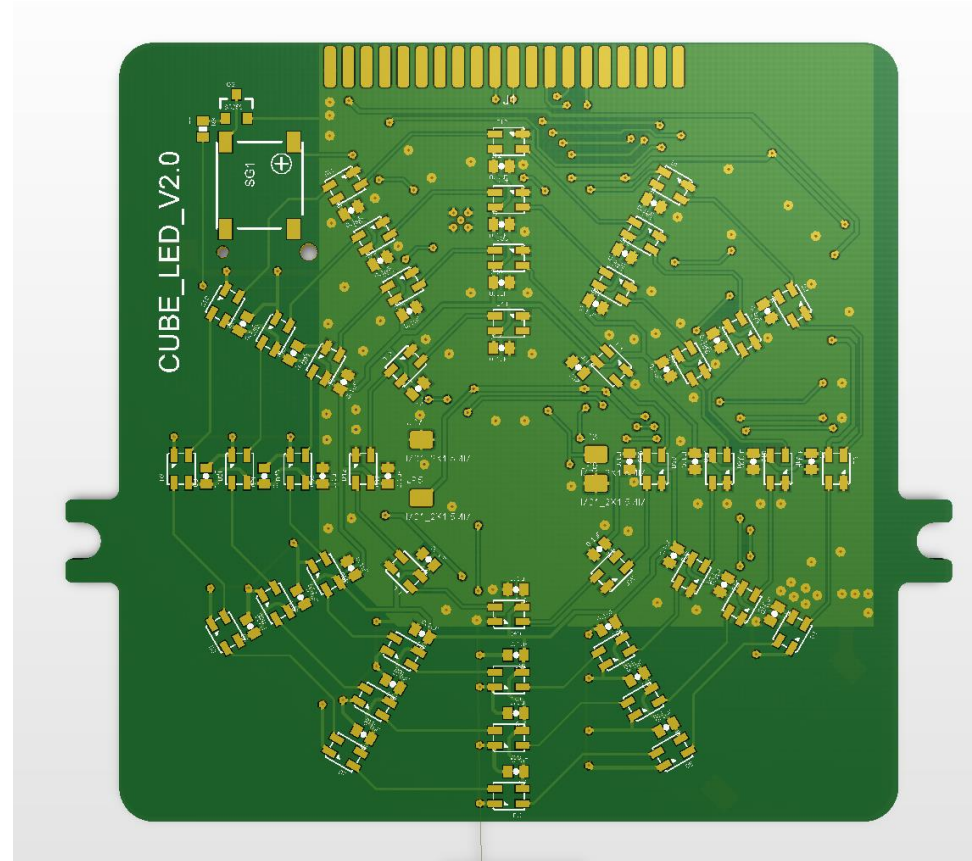
- ❖ Raspberry Pi Zero W
- ❖ USB2514B 4*USB HUB
- ❖ RTL8822BU 2.4G/5.8G WIFI

- ❖ DS1307 RTC
- ❖ SPI Flash
- ❖ Beep
- ❖ MIC

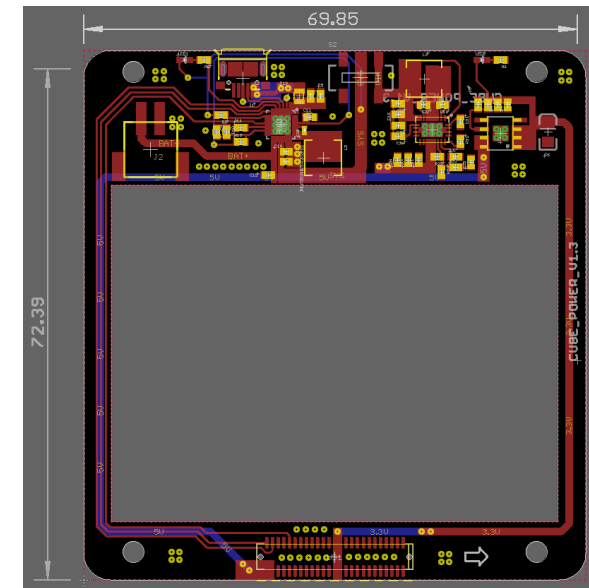
RGB LED and Power Board

- ❖ Arduino Micro Pro 3.3V
- ❖ CC1101 433MHz
- ❖ CC1101 315MHz
- ❖ nRF24L01+ PA

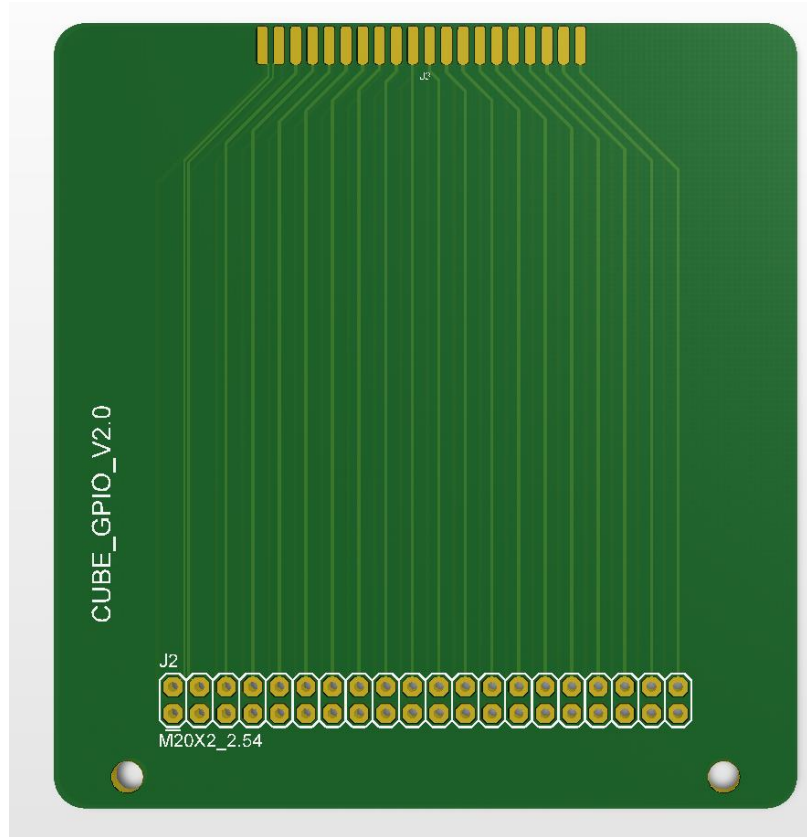
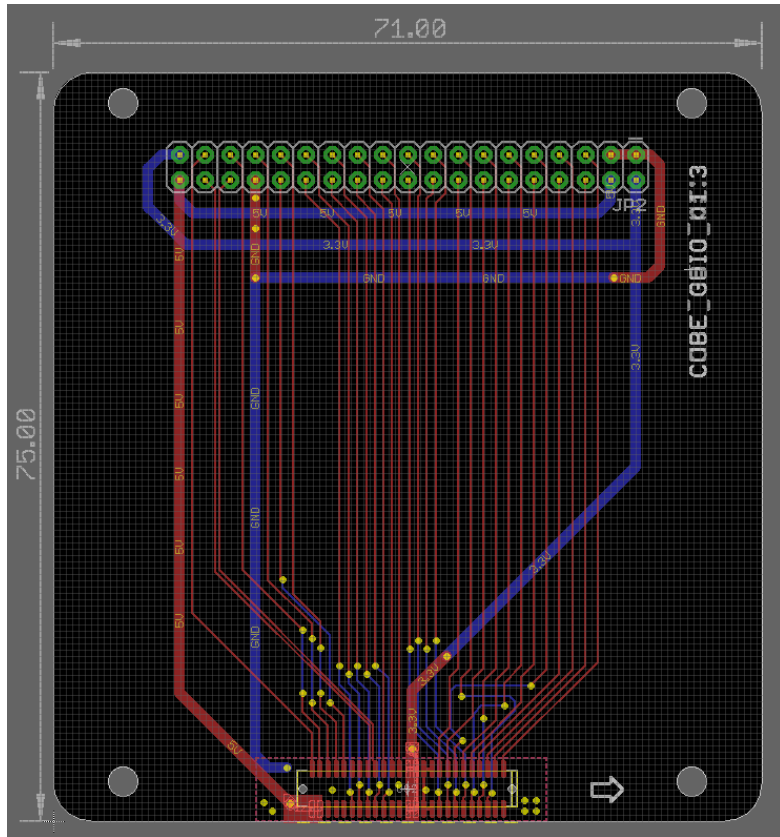
- ❖ Millions RGB LED
- ❖ Show Light
- ❖ Show Logo
- ❖ Flashlight



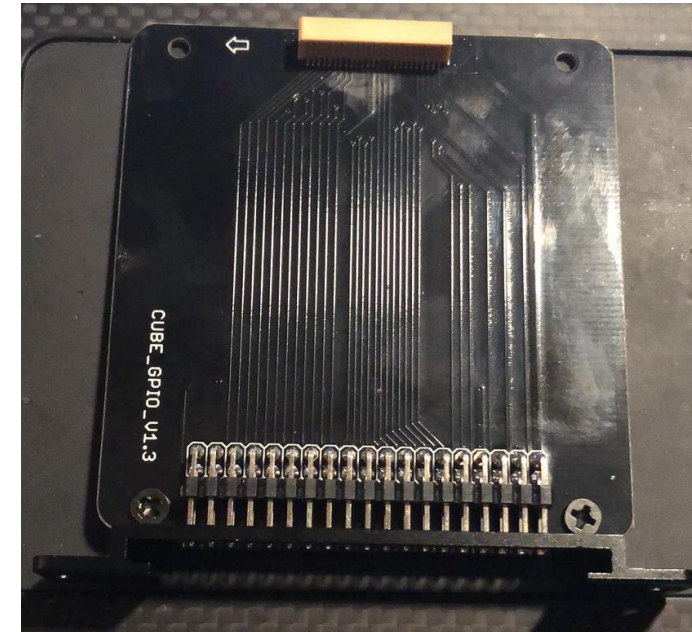
- ❖ TI BQ25895
 - ❖ Supports Max Charge (QC3.0)
- ❖ TI TPS61088
 - ❖ Boost to 5V



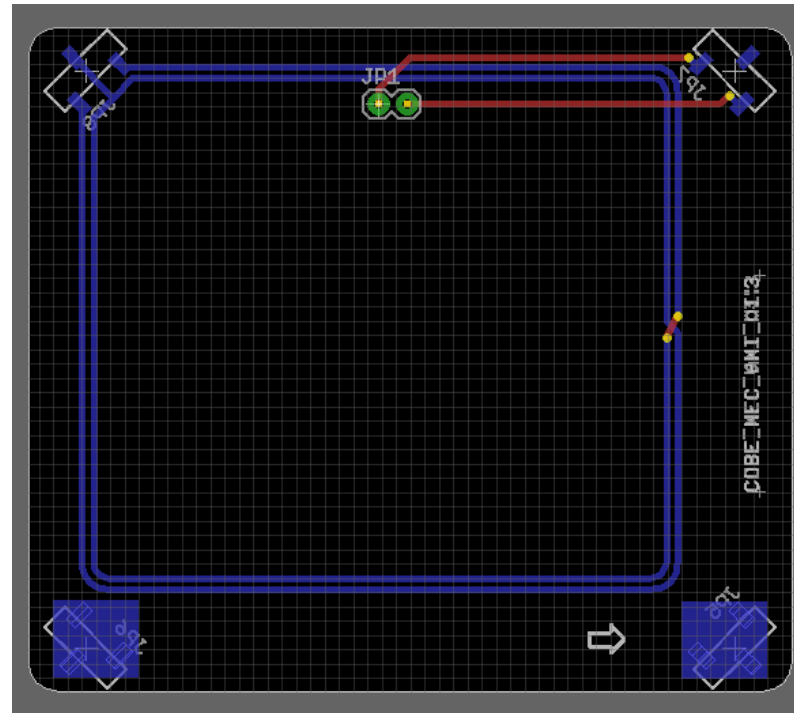
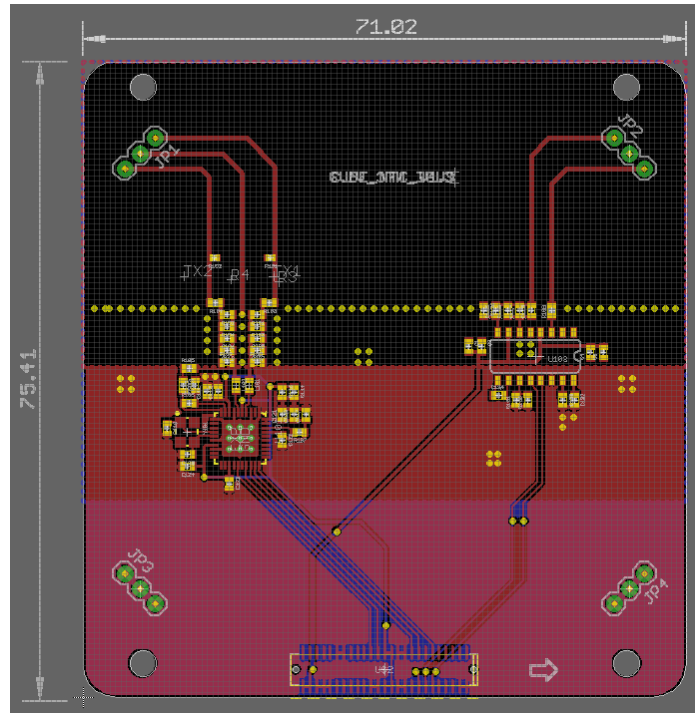
GPIO Extension without Wire



- ❖ Board with GPIO are being extended without wired
- ❖ Neat and Clean Inside

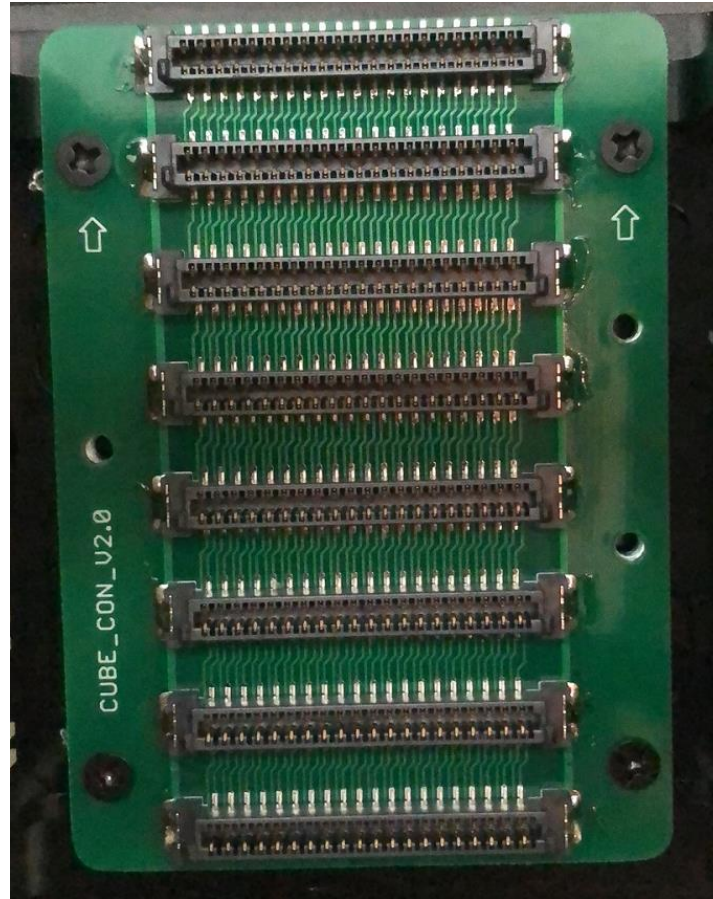
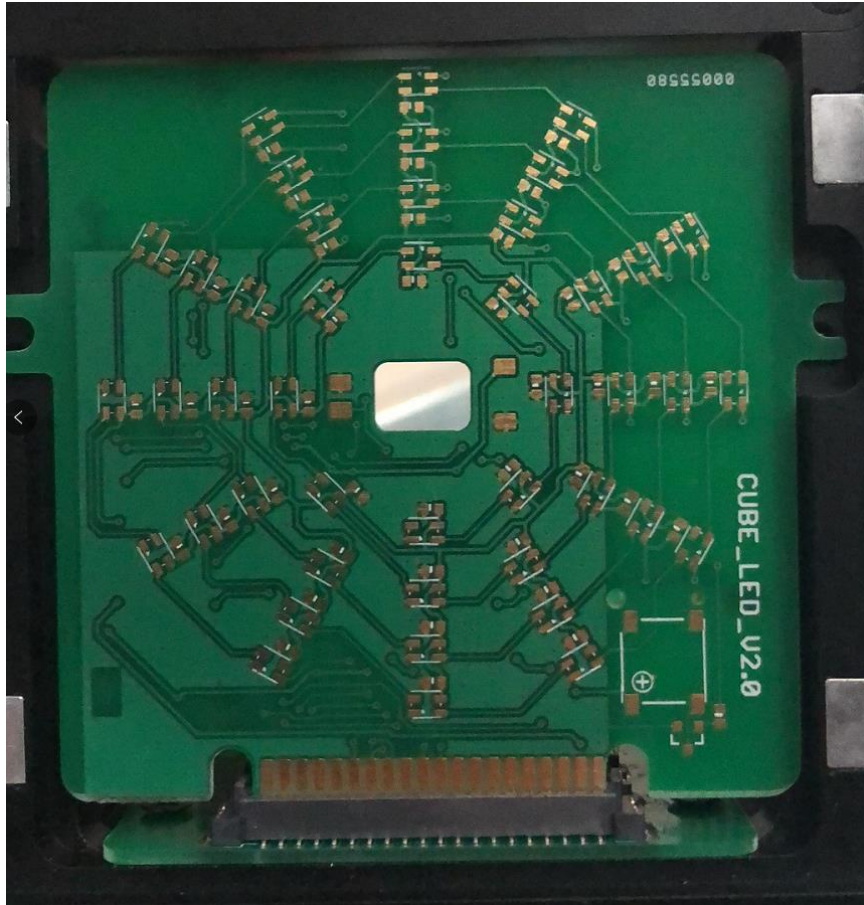


Your Door Access Card

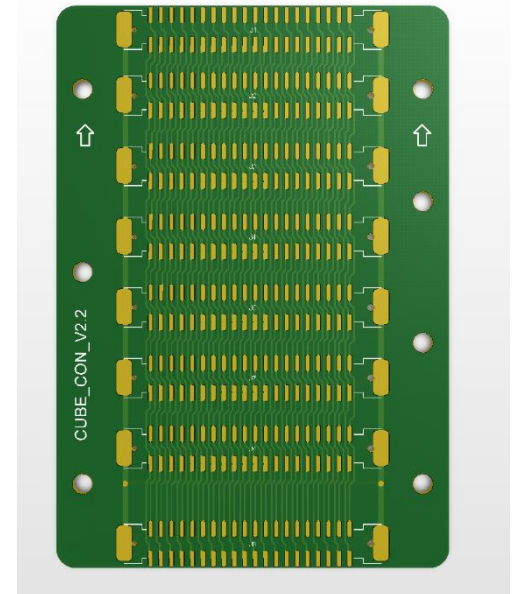


- ❖ PN532
- ❖ EM4095

Zero Wire System




- ❖ 2*20P 0.8mm BTB Connector
- ❖ 8 * Connector
- ❖ Just like your PCI-E Slot



DEMO



Demo 1: Works with Mobile Web Browser



192.168.2.3


Warning! 
This equipment is limited to risk demonstration,
please pay attention to consciously abide by
relevant laws and regulations.

Cube Wifi Manage



Security Risk Detection on 2.4Ghz 5Ghz Devices

WiFi List  

SSID	BSSID	RSSI	JAM
knakworst	08:76:FF:83:2C...	-97	
HackCUBE_30:...	B8:27:EB:30:1E...	-61	



Client List

MAC	BSSID	RSSI	JAM
2C:F0:EE:26:AF:...	None	-65	
8C:85:90:31:E5:B3	None	-109	

- ❖ WIFI AP:
HackCUBE_xx:xx:xx
- ❖ Works with any default
moble web browser
- ❖ Does not work with Some
Playstore or Some
AppStore
- ❖ Save your Notebook at
home

Demo 2: Play RC, with 47MHz



HackCUBE with all possibilities

Demo 3: nRF24L1



HackCUBE with all possibilities

Demo 4: More Realistic Hack



HackCUBE with all possibilities

Demo 5: The Rubber Ducky



HackCUBE with all possibilities

Demo 6: Card Replicator On The Road

Cube NFC Manage
Safety Risk Detection for
Cards Working at 125Khz,
13.5Mhz.

Read 

VID	ID	WRITE	SIMULATE
050	6835882		

Write 

VID

ID

Simulate 

VID

ID

```
nfc-list uses libnfc 1.7.1
NFC device: pn532_spi:/dev/spidev0.0 opened
1 ISO14443A passive target(s) found:
ISO/IEC 14443A (106 kbps) target:
  ATQA (SENS_RES): 00 04
  UID (NFCID1): 0a 1a cd 09
  SAK (SEL_RES): 08
```

Cube NFC Manage
Safety Risk Detection for
Cards Working at 125Khz,
13.5Mhz.

Read 

VID	ID	WRITE	SIMULATE
050	6835882		

Write 

VID

ID

Simulate 

VID

ID

```
nfc-list uses libnfc 1.7.1
NFC device: pn532_spi:/dev/spidev0.0 opened
1 ISO14443A passive target(s) found:
ISO/IEC 14443A (106 kbps) target:
  ATQA (SENS_RES): 00 04
  UID (NFCID1): ce 79 4f 3f
  SAK (SEL_RES): 08
```

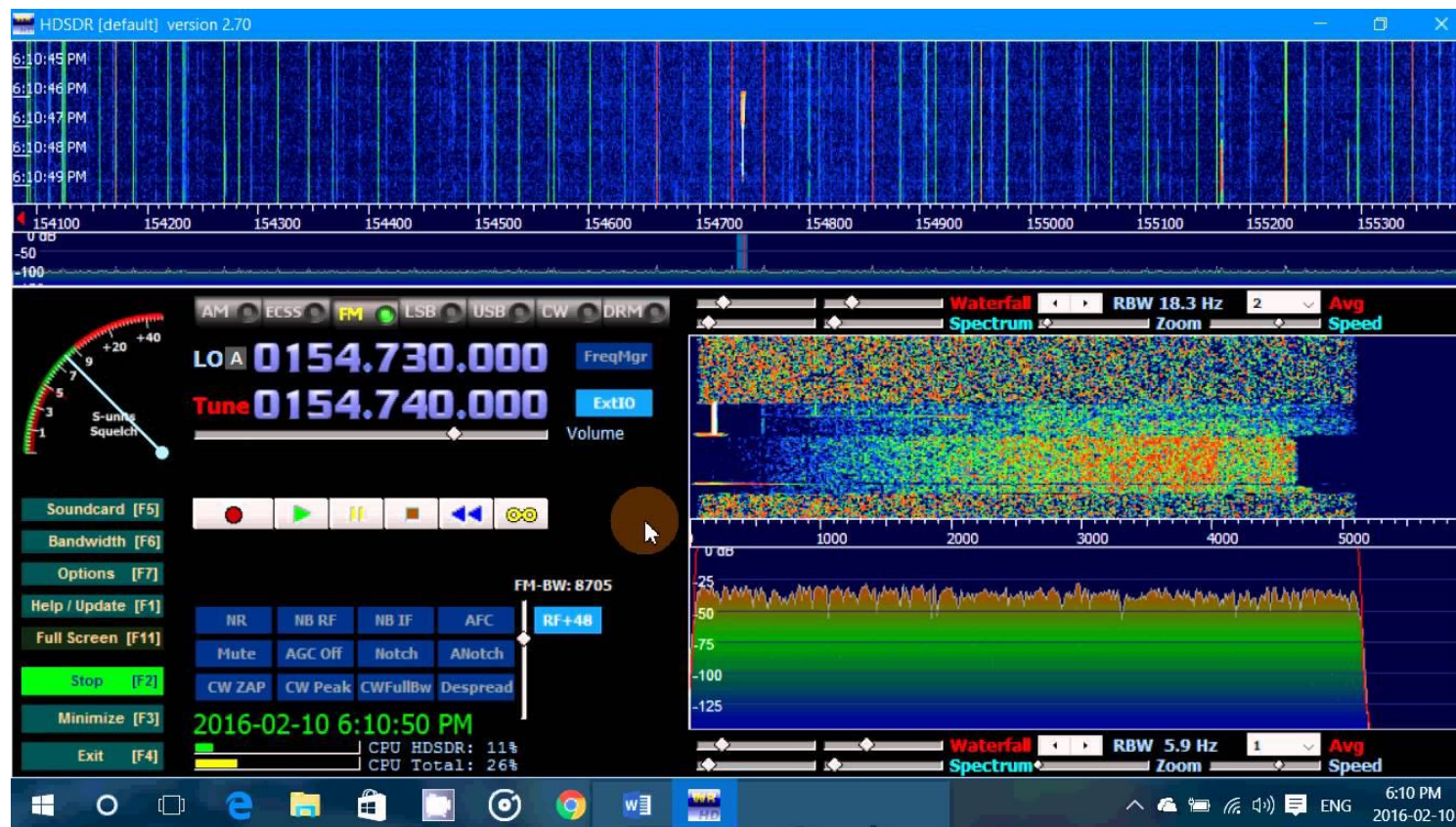
- ❖ To Read
- ❖ To Write
- ❖ To Emulate
 - ❖ 125Khz Card
 - ❖ 13.5 Mhz Card

Demo 7: LED Playing Time

Not a toy after all

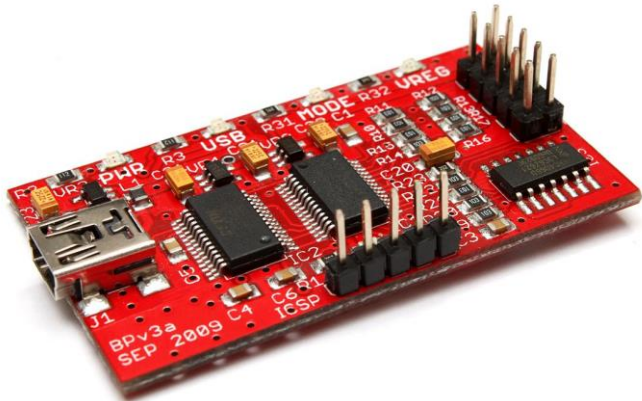
What Next

SDR



RTL2832U Integration or HackRF One

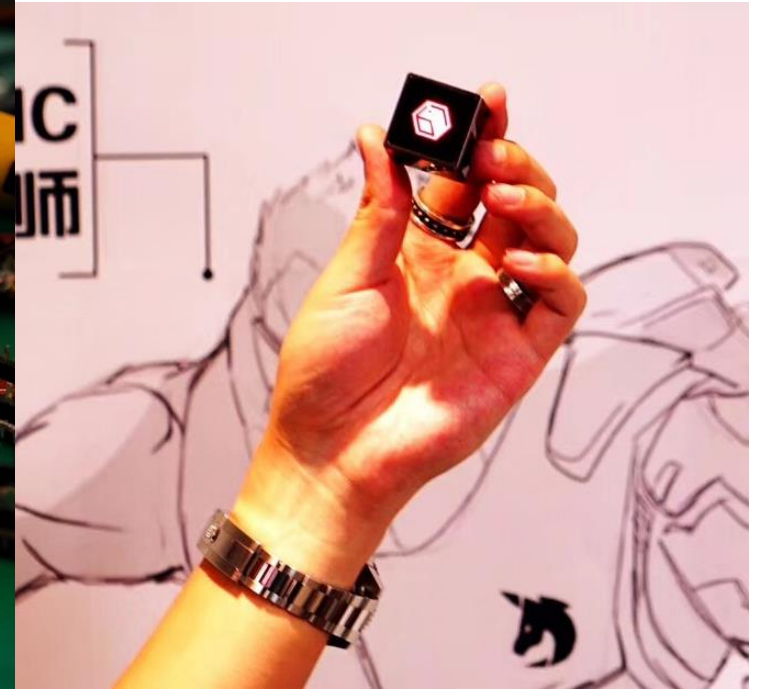
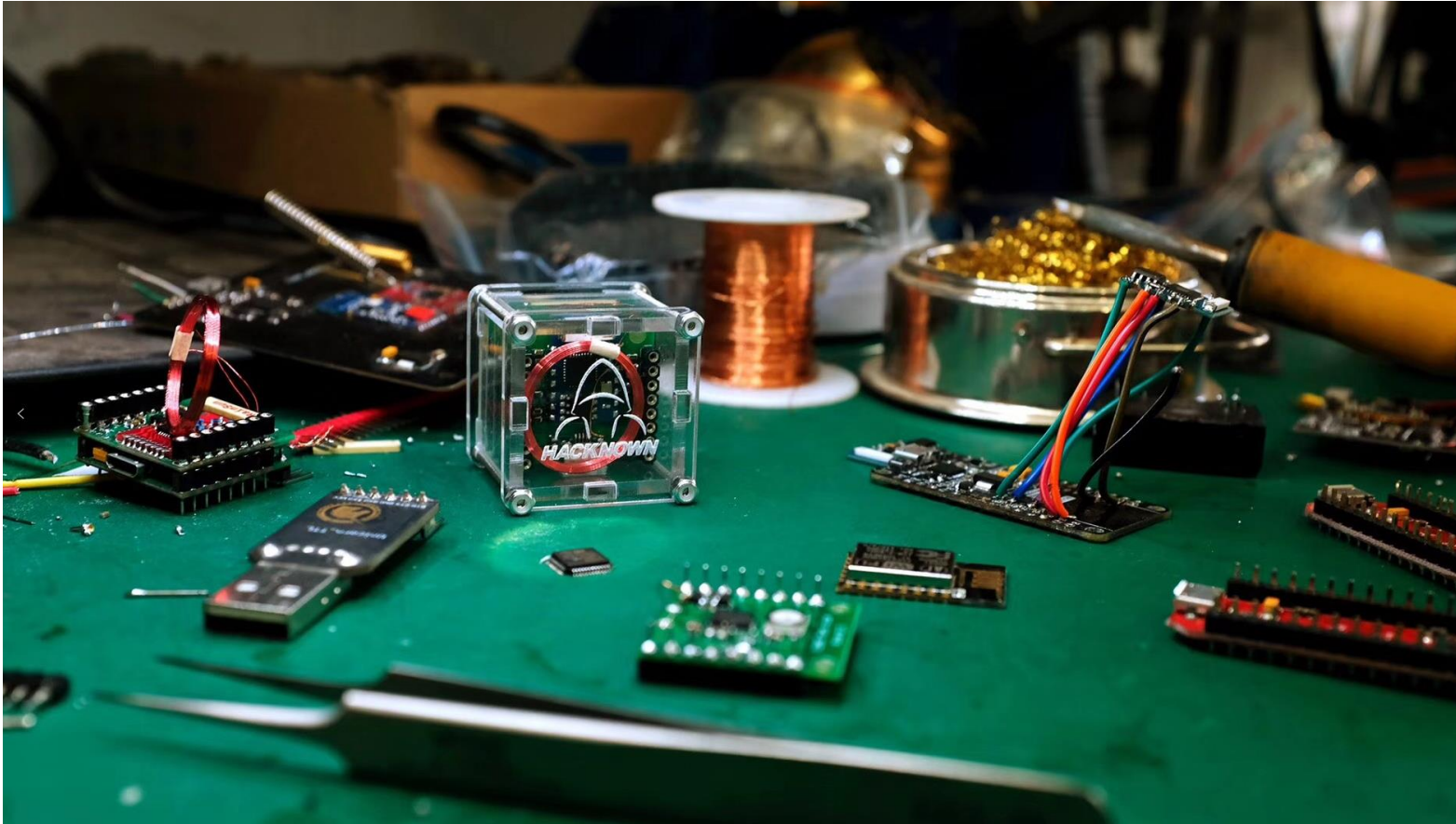
Something Not For Everyone



- ❖ OpenJTAG
- ❖ Buspirate
- ❖ CC Debugger
- ❖ Logic Analyzer
- ❖ IR Analyzer
- ❖ CAN Bus Aalyzer
- ❖ Zigbee Sniffer
- ❖ BLE Sniffer
- ❖ Other ...

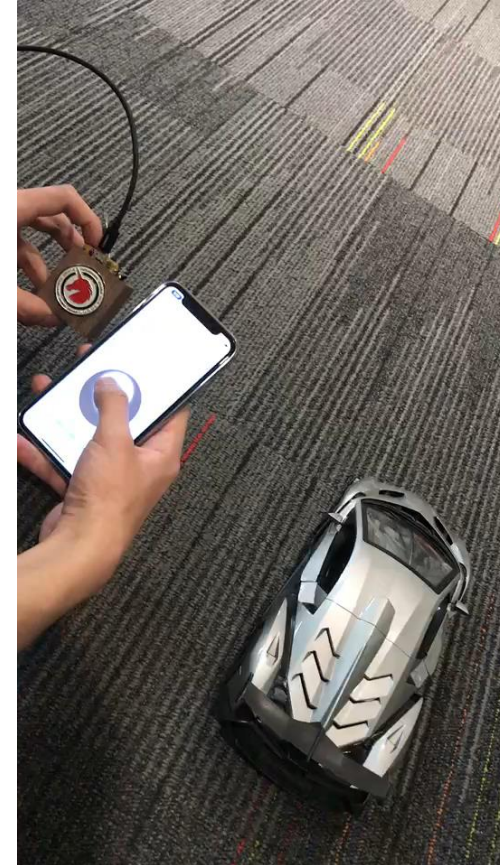
If HackCUBE is HUGE

Working in Progress



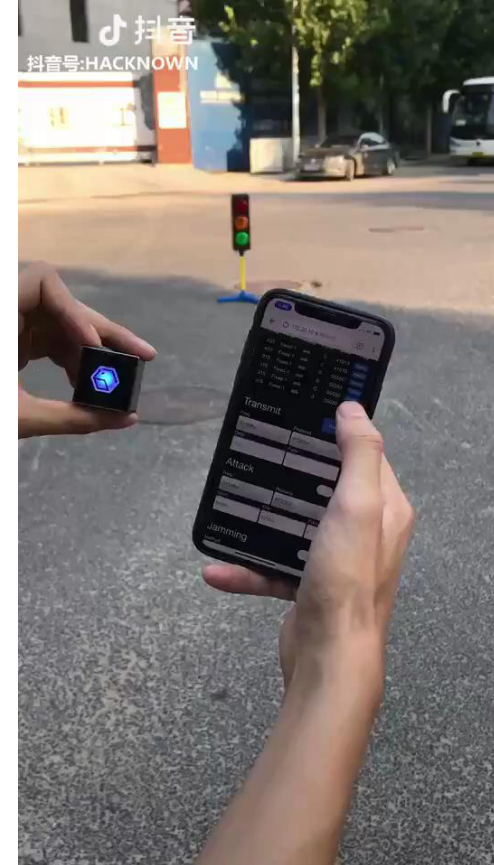
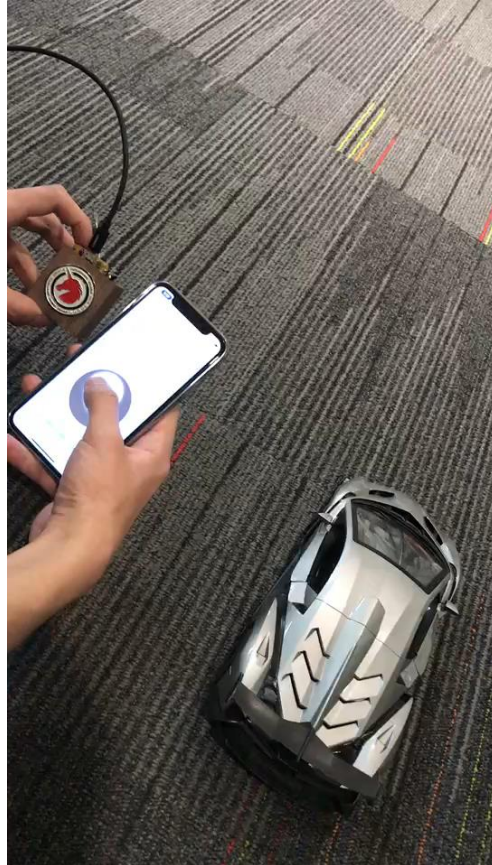
Smaller, Portable and Cheaper, Just like somePHONE XS

HackCUBE Mini



Smaller, Portable and Cheaper, Just like somePHONE XS

HackCUBE Mini



Smaller, Portable and Cheaper, Just like somePHONE XS

HackCUBE Mini



Smaller, Portable and Cheaper, Just like somePHONE XS

HackCUBE Mini



Smaller, Portable and Cheaper, Just like somePHONE XS

Just in case I am too Lazy, Where to Buy

Reach US @

@sgniwx



@WhiteA10n3



<https://github.com/UnicornTeam/hackcube.git>



**“YOU TALK
TOO MUCH.”**

#THEBLACKLIST

QUESTIONS