Using IoT devices as Attack Vectors

Available at:https://bruce.computer/presentation.pdf

DISCLAIMER 😇

Bruce is a tool for penetration testing operations and RedTeam activities, distributed under the terms of the Affero General Public License (AGPL). It is intended exclusively for legal and authorized security testing purposes. The use of this software for any malicious or unauthorized activities is strictly prohibited.

What can we do with a ESP32?

Probably you are familiar or have seen some devices from Espressif, we can also include modules on it to make a infinity of attacks, but by default the mayority of the ESPs lets you handle 2.4Ghz networks such as Wi-Fi and Bluetooth (LE), a lot of automations are possible with it but there is so much attacks we can do in these also.
Also these devices are so tiny and cheap you can let it somewhere and come back, or never come back

XIAO ESP32C3:

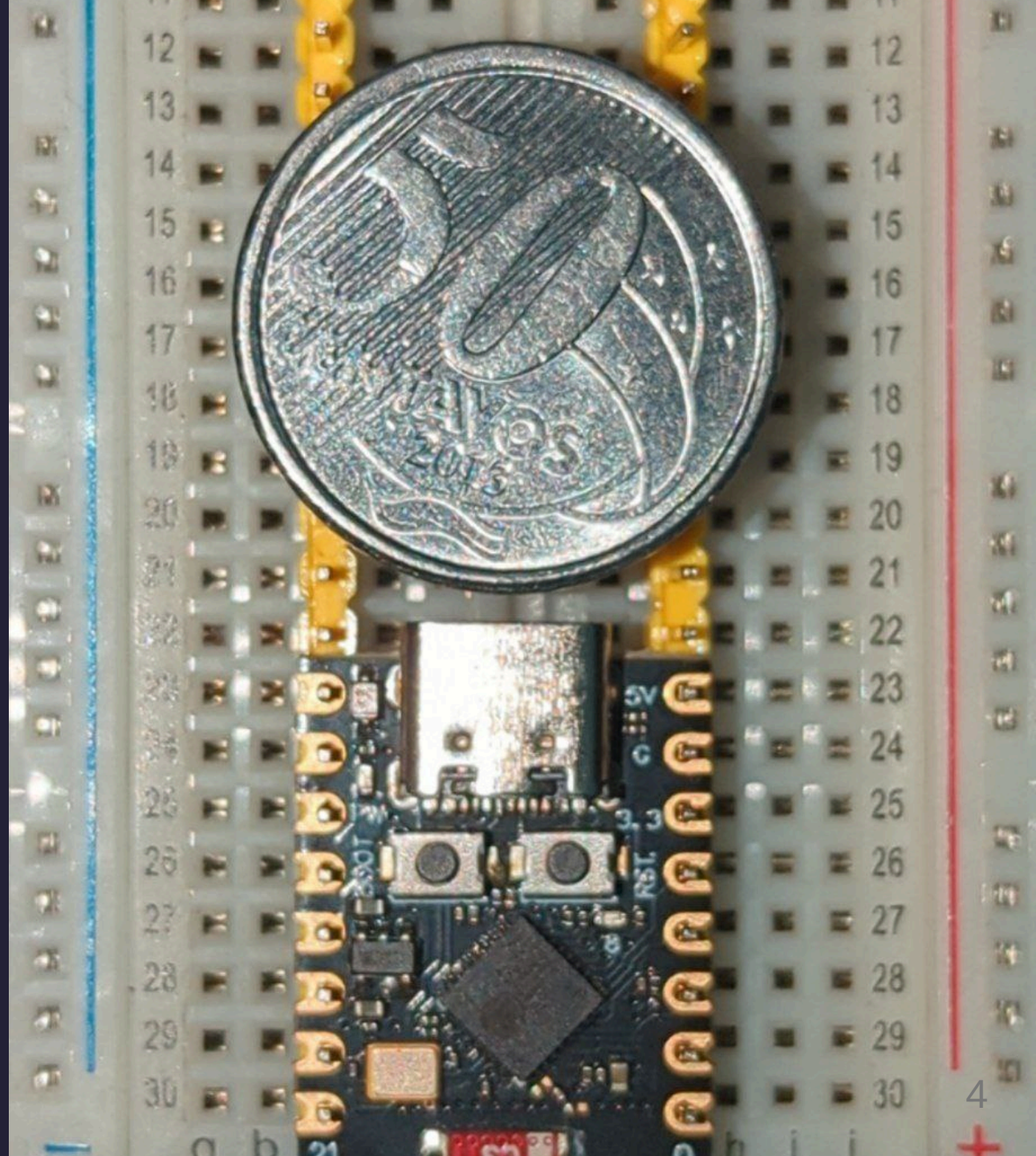
- Dimensions: 21 x 17.5 x 3.5 mm

ESP32-S3 Super Mini (USB HID):

- Dimensions: 22.52 x 18 x 2.54 mm

ESP32-C5-WROOM-1U-N8R4:

- Dimensions: 18.0 × 21.2 × 3.3 mm



ESPs on 5Ghz

> ESP32-C5 2.4/5GHz

< ESP32-S5 2.4GHz

Wi-Fi attacks (not authenticated)

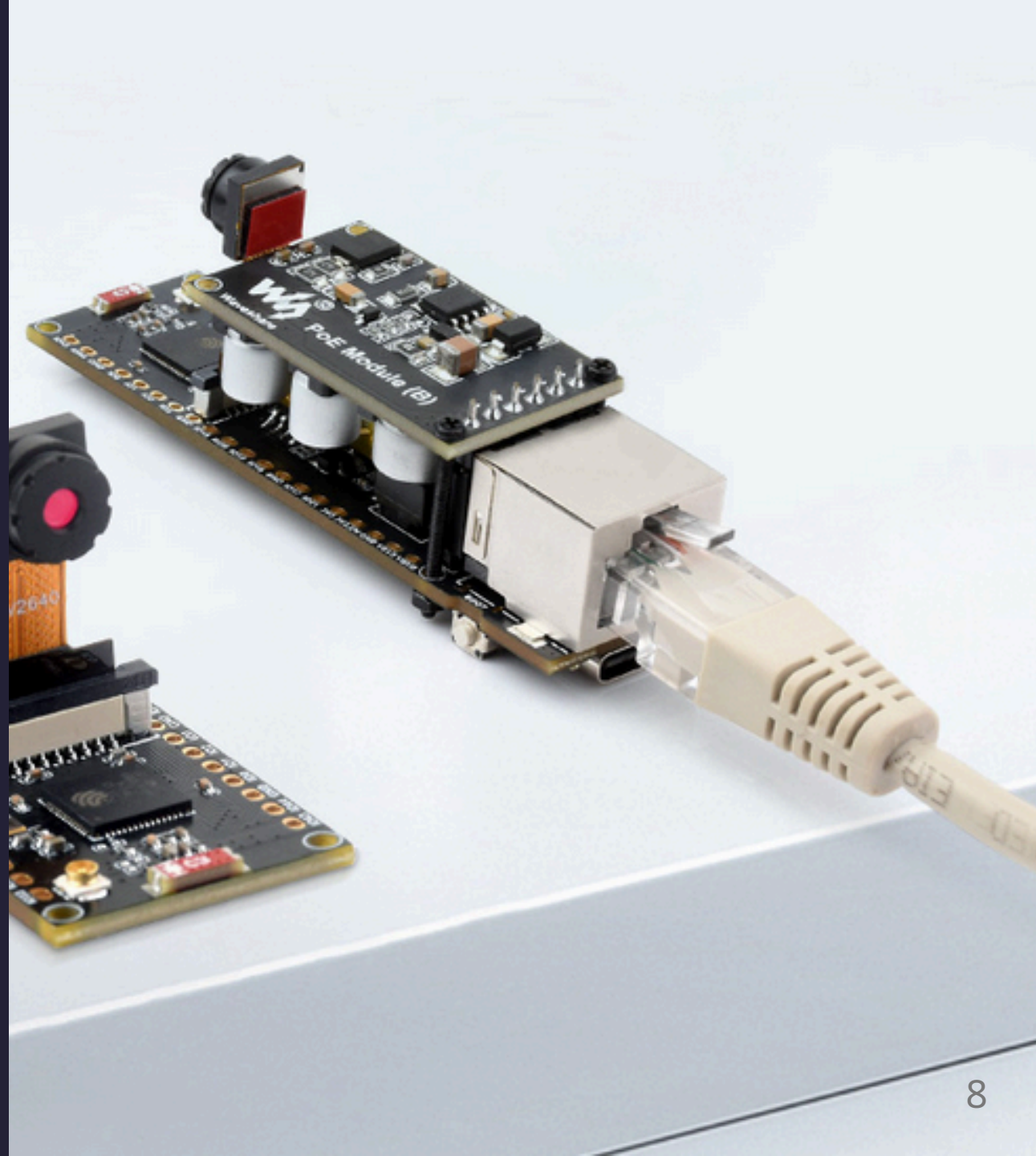
- Colect EAPOL Handshakes
- Evil Twin
- KARMA attacks
- PEAP Relay Attack (MGT)
- WPS Pixie Dust
- DPWO or any router exploit

Authenticated Network attacks

If you are inside a network, one of the first things you would do is discover other hosts. The technique you gonna use depends on how many "noise" you can/want to make.

Organization

- LLMNR Poisoning (responder)
- ARP Spoofing
- DNS Spoofing
- DHCP Poisoning
- Bruteforce
- Scan Hosts range (TCP/UDP)
- Weak Cryptografy



Available at:https://bruce.computer/presentation.pdf

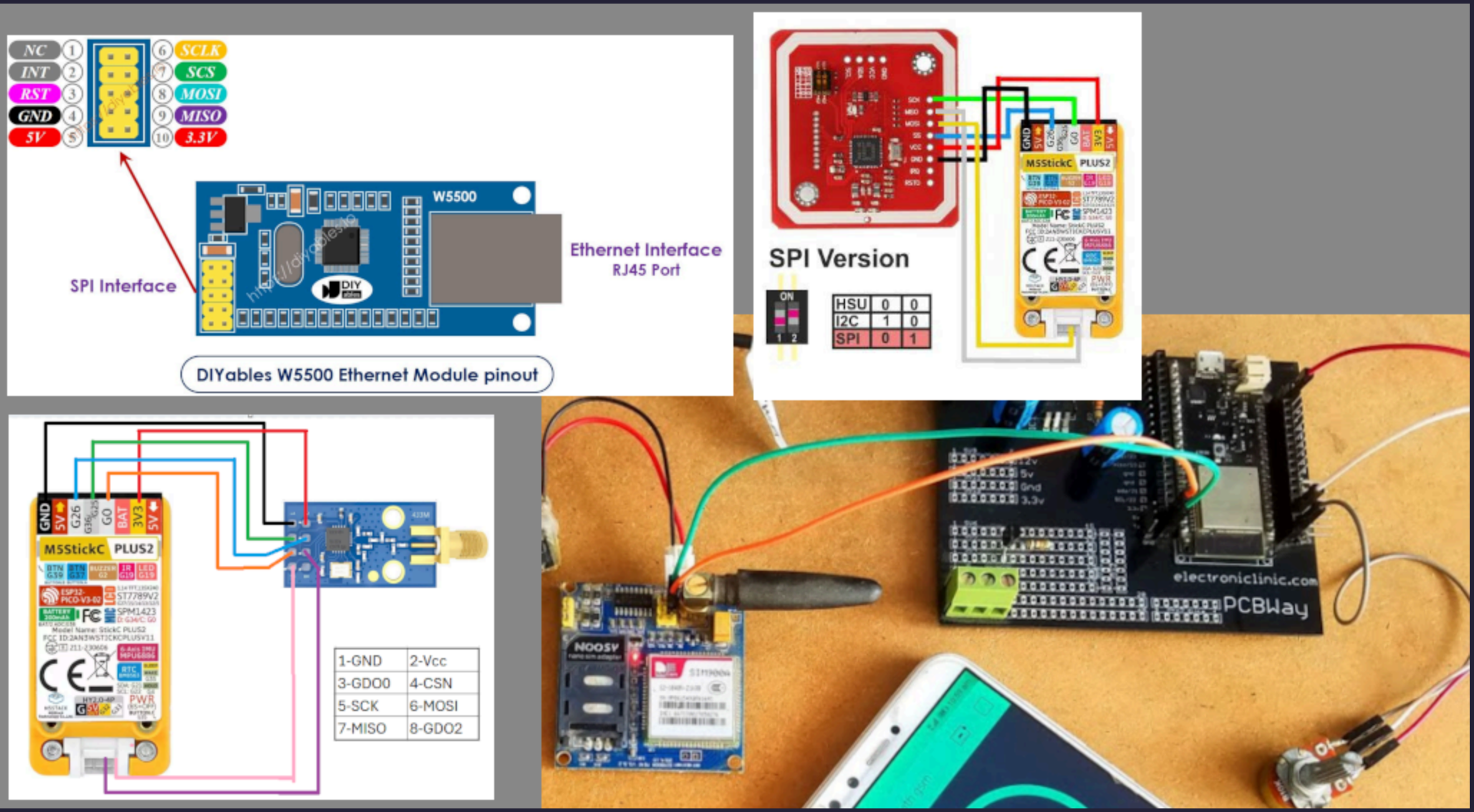
Bluetooth

ESP32-S3 suports Bluetooth 5.0 (LE) and its certificated for Bluetooth LE 5.4.

- Openhaystack/Device tracking
- Bluejacking
- BLE Spoofing
- Passive eavesdropping

Customizing the ESP32

- SIM-900A
- CC1101
- PN532
- W5500


NC 1
INT 2
RST 3
GND 4
5V 5
6 SCLK
7 SCS
8 MOSI
9 MISO
10 3.3V
W5500
SPI Interface
Ethernet Interface
RJ45 Port
DIYables W5500 Ethernet Module pinout
SPI Version
ON
1 2
HSU 0 0
I2C 1 0
SPI 0 1
M5StickC PLUS2
1-GND 2-Vcc
3-GDO0 4-CSN
5-SCK 6-MOSI
7-MISO 8-GDO2
electroniclinic.com
PCBWay

RF (SubGhz)

- Scan/Copy to file
- Send frequencies from files
- Spectrum

RFID

- Read tag
- Read 125kHz
- Clone tag
- Write NDEF records
- Amiibolink
- Chameleon
- Write data
- Erase data
- Save file
- Load file

Hardware vulns

TP-Link RE305

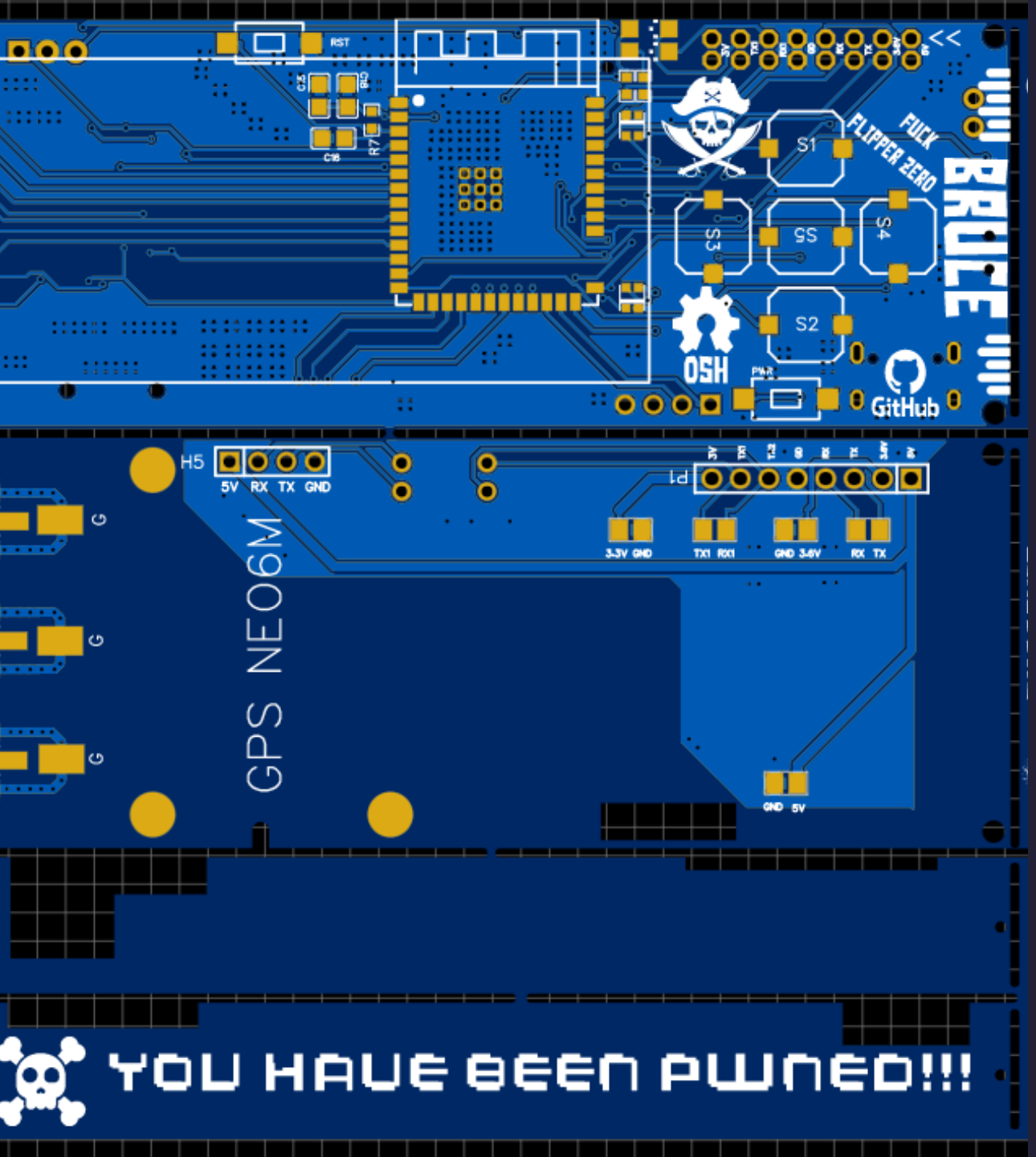
Available at:https://bruce.computer/presentation.pdf

Install it everywhere

If it has a ESP32, you can install Bruce someway

kawai ca701

Available at:https://bruce.computer/presentation.pdf



True Open Source hardware!

https://bruce.computer/boards

CERN-OHL-P-2.0 License

Available at:https://bruce.computer/presentation.pdf

How i get rid of it?

- Dont use weak passwords (Use password manager)
- Avoid connecting on WiFi you dont trust
- Monitor your network and use DNSSEC (use too VLANs)
- Dont auto-connect to Wi-Fi
- Use controls with rolling key
- Use only WPA3 without WPS

Getting Started

Ok, Lets go!

The firmware recording of Bruce on the board can be done through the website https://bruce.computer/flasher

You can also install Bruce using the Official Bruce App for Android via USB OTG! (Soon on playstore and Fdroid)

Flashing the board

1. Go to https://bruce.computer/flasher

Flashing the board

2. Select “Cardputer” (or any other device)

Flashing the board

3. After clicking in *“Connect”* and *"Install"* we are done!

Greetz/Gracias

andres, saico, mini and all Phacker org!

bmorcelli, IncursioHack e r3ck!

All the Bruce community!

Espressif, M5stack, Lilygo, Elecrow and PCBWay!

References

- https://github.com/pr3y/bruce/wiki
- https://github.com/engn33r/awesome-bluetooth-security
- https://docs.espressif.com/projects/esp-idf/en/stable/esp32s3/api-guides/ble/overview.html
- https://sensepost.com/blog/2015/improvements-in-rogue-ap-attacks-mana-1%2F2/
- https://github.com/s0lst1c3/eaphammer
- https://www.allaboutcircuits.com/technical-articles/vulnerabilities-and-attacks-on-bluetooth-le-devicesreviewing-recent-info/
- https://sensepost.com/blog/2019/peap-relay-attacks-with-wpa_sycophant/

- https://github.com/lgandx/Responder
- https://github.com/7h30th3r0n3/Evil-M5Project
- https://github.com/geo-tp/ESP32-Bus-Pirate
- https://github.com/caioluders/DPWO
- https://github.com/Zero-Sploit/FlipperZero-Subghz-DB
- https://openwrt.org/