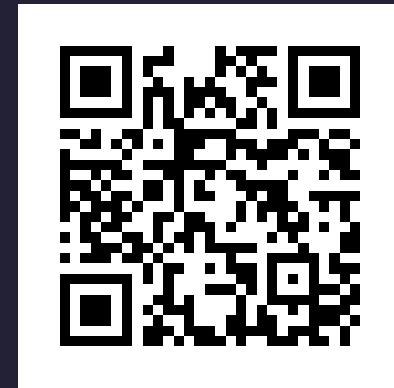


Utilização de dispositivos IoT como vetores de ataques



DISCLAIMER 😊

Bruce é uma ferramenta para operações de testes de intrusão e atividades de RedTeam, distribuída sob os termos da Licença Pública Geral Afferro (AGPL). É destinada exclusivamente para fins legais e autorizados de testes de segurança. O uso deste software para quaisquer atividades maliciosas ou não autorizadas é estritamente proibido.

O que podemos fazer com um ESP32?

Vocês provavelmente já estão bem familiarizados com os dispositivos da Espressif, podemos também sempre usar mais módulos para uma infinidade de ataques, porém por padrão a maioria dos ESP32 nos concede acesso a redes 2.4Ghz (Wi-Fi) e Bluetooth (LE), além de várias automações serem possíveis aonde não eram antes, podemos também fazer qualquer ataque nesses vetores por padrão!

Podemos deixar em um lugar e voltar ou nunca mais voltar!

XIAO ESP32C3:

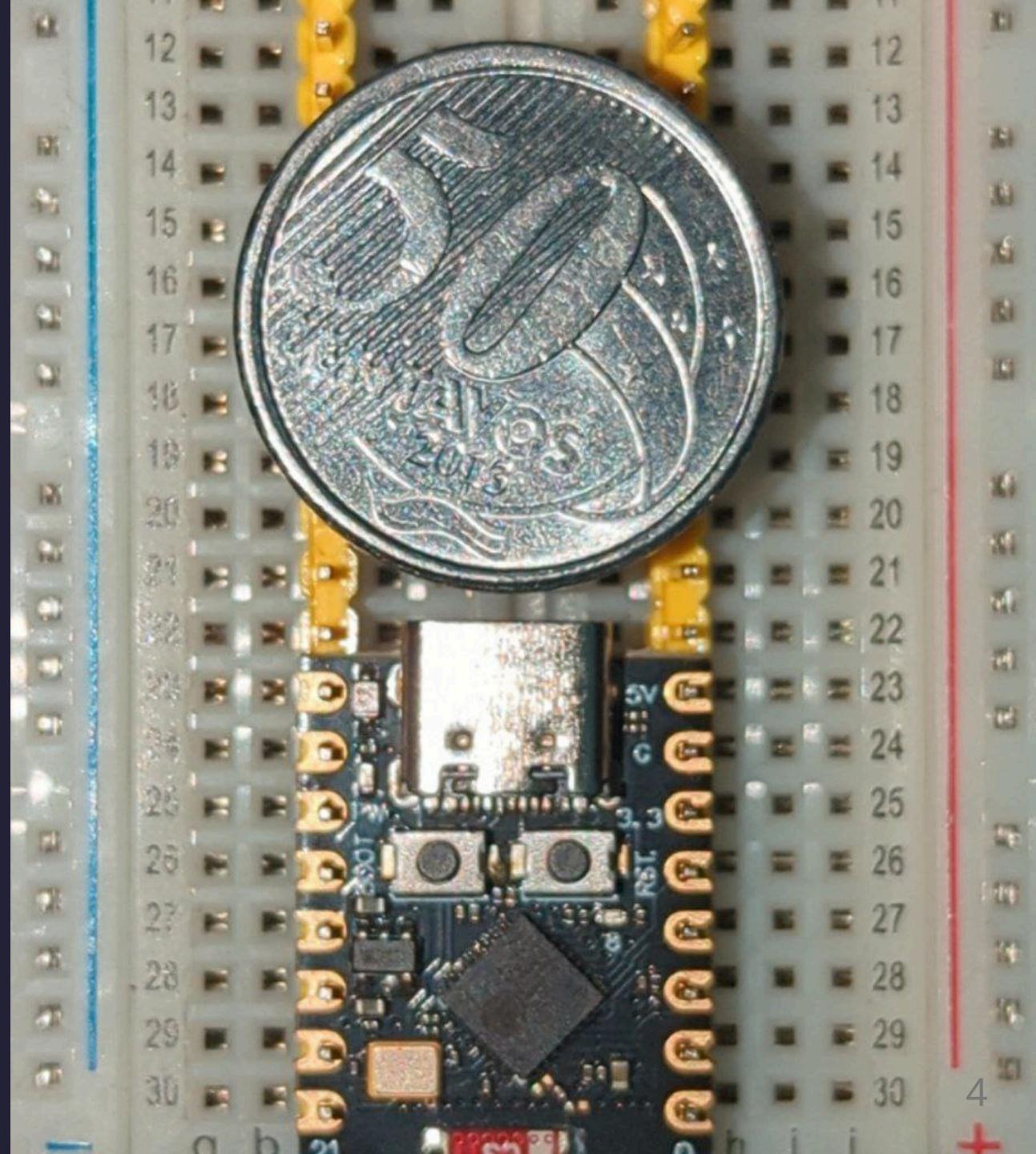
- Dimensões: 21 x 17.5 x 3.5 mm

ESP32-S3 Super Mini (USB HID):

- Dimensões: 22.52 x 18 x 2.54 mm

ESP32-C5-WROOM-1U-N8R4:

- Dimensões: 18.0 × 21.2 × 3.3 mm



Qual dispositivo usar?

> **ESP32-C5 2.4/5GHz**

< **ESP32-S5 2.4GHz**

ESP32-P4 tem ethernet

Ataques em redes Wi-Fi (não autenticado)

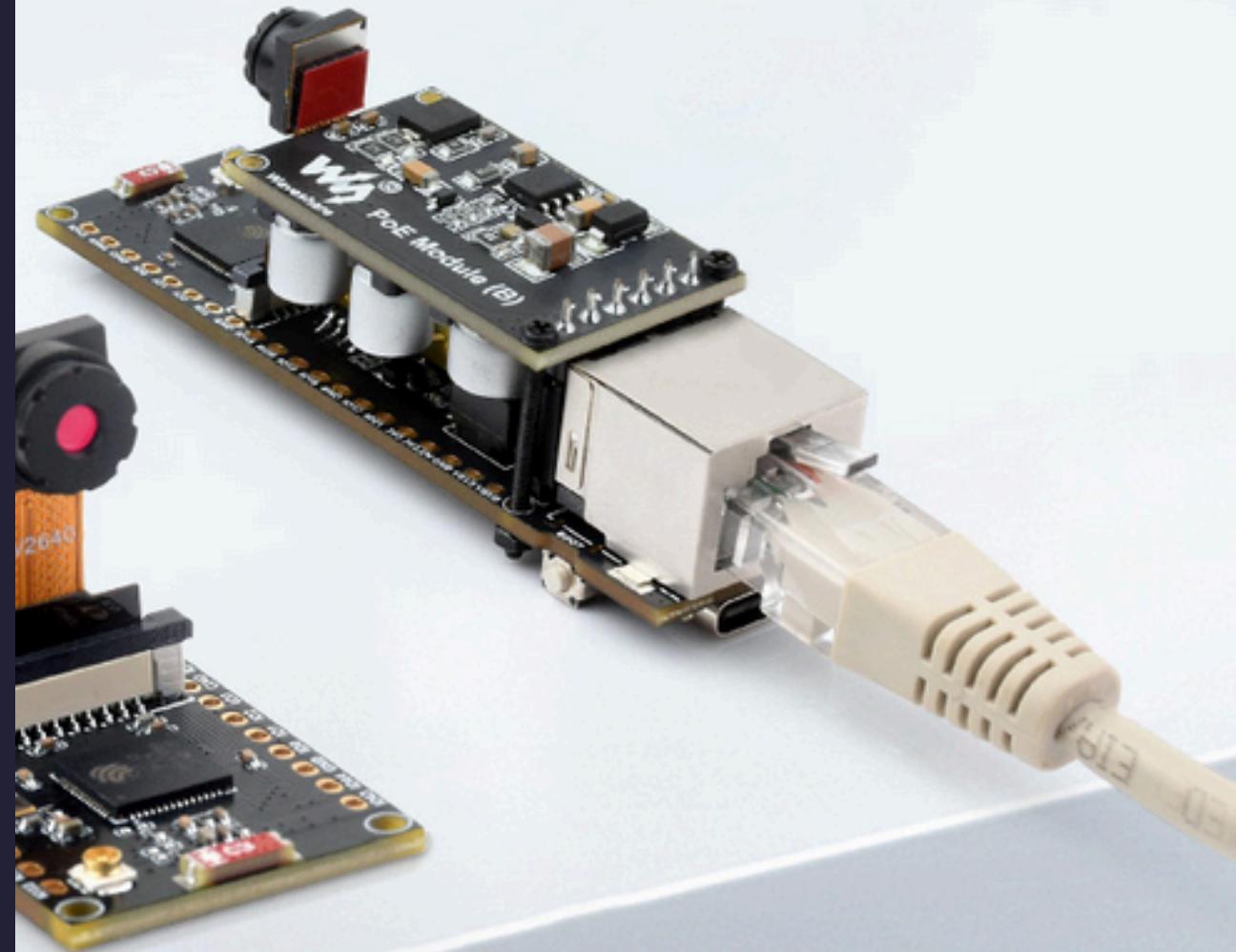
- Coletar Handshakes EAPOL
- Evil Twin
- KARMA attacks
- PEAP Relay Attack (MGT)
- WPS Pixie Dust
- DPWO ou qualquer exploit de roteador

Ataques em redes (autenticado)

Se você está dentro de uma rede, uma das primeiras coisas que vai querer fazer será descobrir outros hosts. Isso também depende de quanto barulho pode/quer fazer.

Organização

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



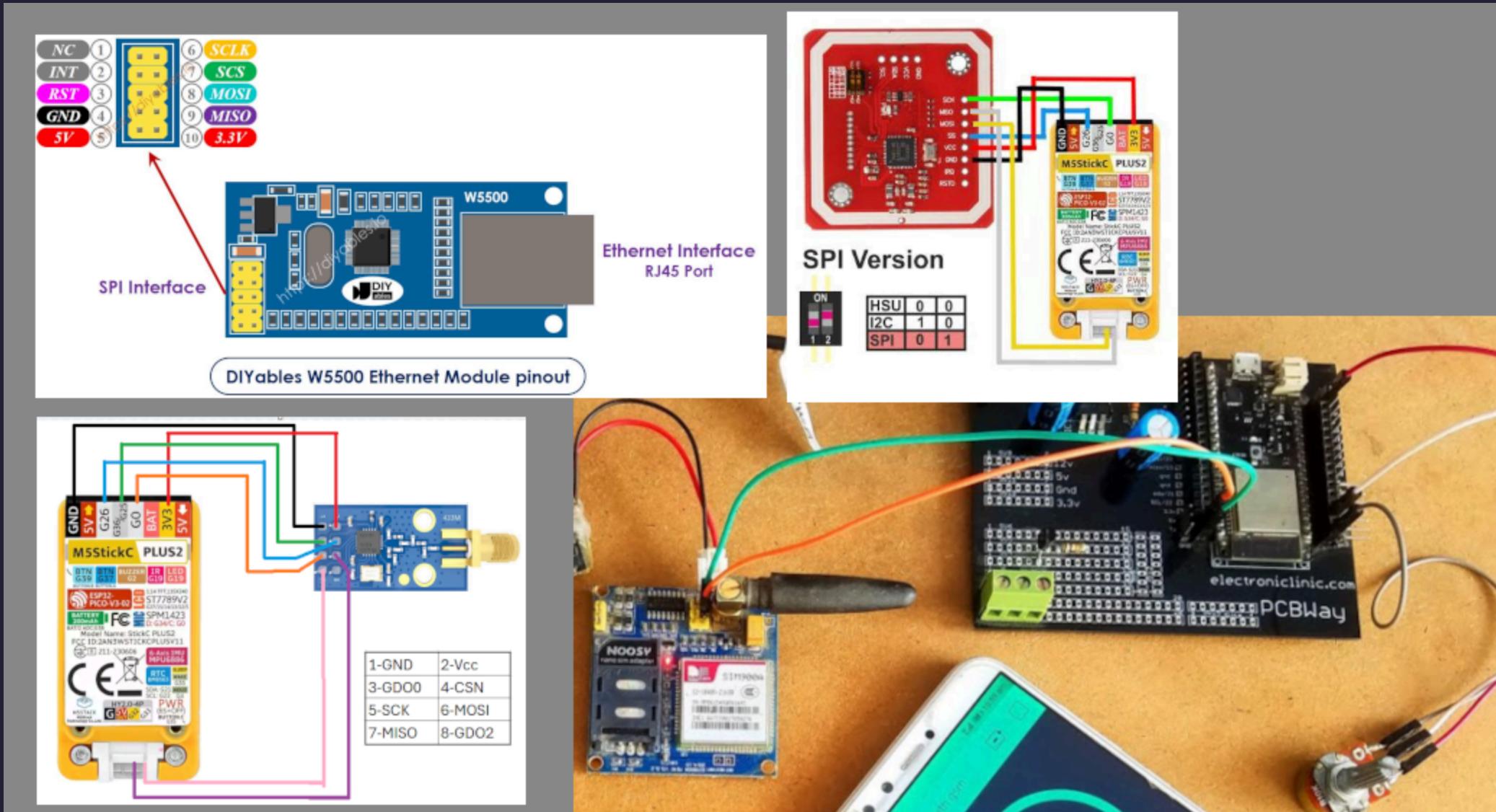
Bluetooth

ESP32-S3 suporta Bluetooth 5.0 (LE) e é certificado para Bluetooth LE 5.4.

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

Customizando o ESP32

- SIM-900A
- CC1101
- PN532
- W5500
- NRF24



RF (SubGhz)

- Scan/Copy para arquivo
- Enviar frequências de arquivos
- Spectrum

RFID

RFID 13.56MHz

M5Stack RFID2 module

MFRC-522 - via I2C

PN532 - via I2C, SPI, or BLE

RFID 125kHz

RDM6300

- Escrever NDEF records
- Amiibolink
- Chameleon

Hardware vulns

TP-Link RE305

Disponível em: <https://bruce.computer/apresentacao.pdf>





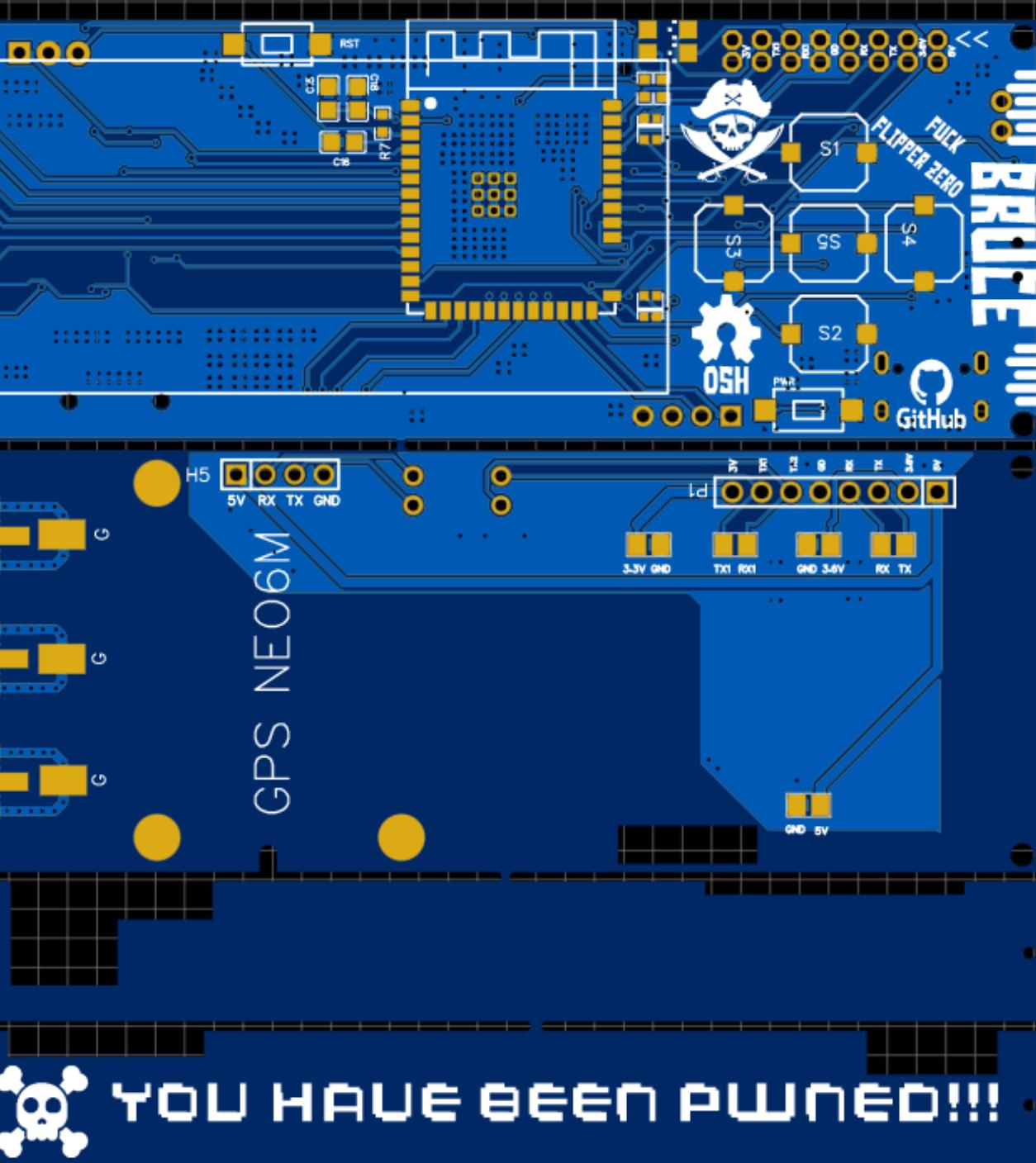
Instale em todo lugar

**Se tem um ESP32, você pode
instalar Bruce**

kawai ca701

Como me livro disso?

- Não use senhas fracas (Gerenciador de senhas)
- Não conecte em Wi-Fi alheio
- Monitore sua rede, use DNSSEC e VLANs
- Não conecte-se automaticamente
- Use controles com rolling key
- Use somente WPA3 sem WPS



True Open Source
hardware!

<https://bruce.computer/boards>

CERN-OHL-P-2.0 License

Como instalar Bruce

**A gravação do firmware Bruce na placa é feita através do site
<https://bruce.computer/flasher>**

**Ou utilizando o App android com o dispositivo via USB OTG
<https://github.com/BruceDevices/App>**

**Todo o código-fonte do firmware esta em
<https://github.com/BruceDevices/firmware>**



Disponível em: <https://bruce.computer/apresentacao.pdf>

Agradecimentos

bmorcelli, IncursioHack e r3ck!

Toda a comunidade Bruce!

Espressif, M5stack, Lilygo, Elecrow and PCBWay!

Referências Gerais

- <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-manage/>
- <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://products.espressif.com/static/Espressif SoC Product Portfolio.pdf>
- <https://github.com/caioluders/DPWO>
- <https://github.com/Zero-Sploit/FlipperZero-Subghz-DB>
- <https://openwrt.org/>
- <https://products.espressif.com/#/product-comparison?type=SoC&names=>