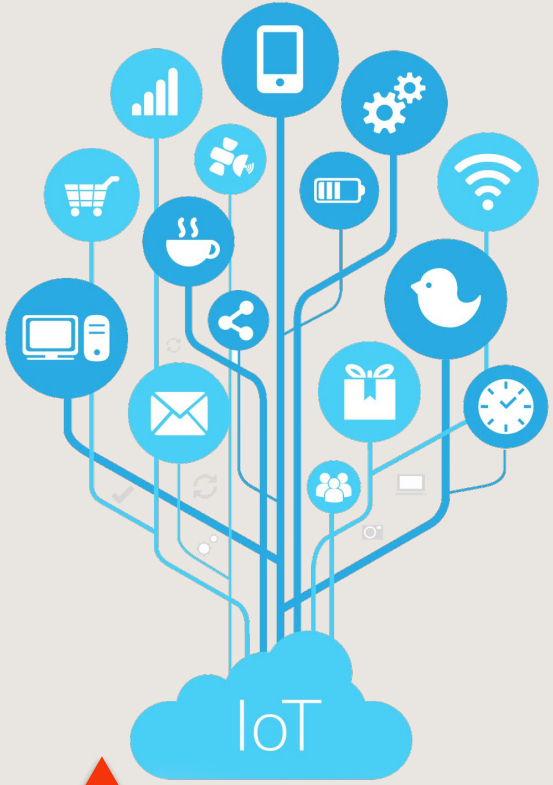
Hardware toolkits for IoT security analysis



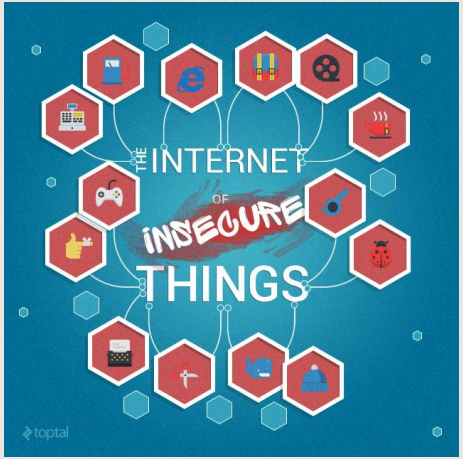
#WHOAMI

Shaposhnikov Ilya

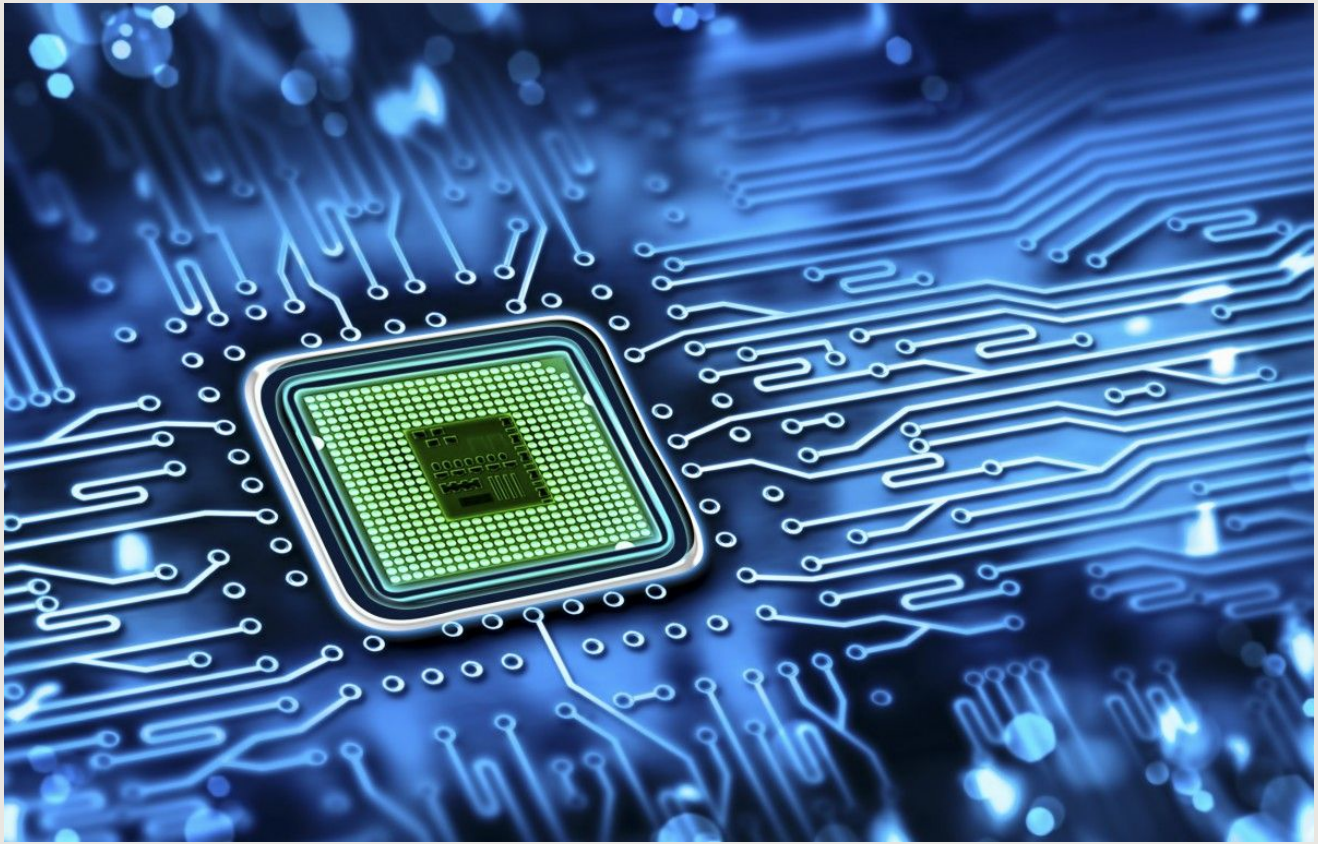
- **SFT0 CTF team member**
- **Invuls SecTeam capitan**
- **Security Expert, RedTeam, Rostelecom**
- **BMSTU student**
- **IoT Security Researcher**

DEFCON NN

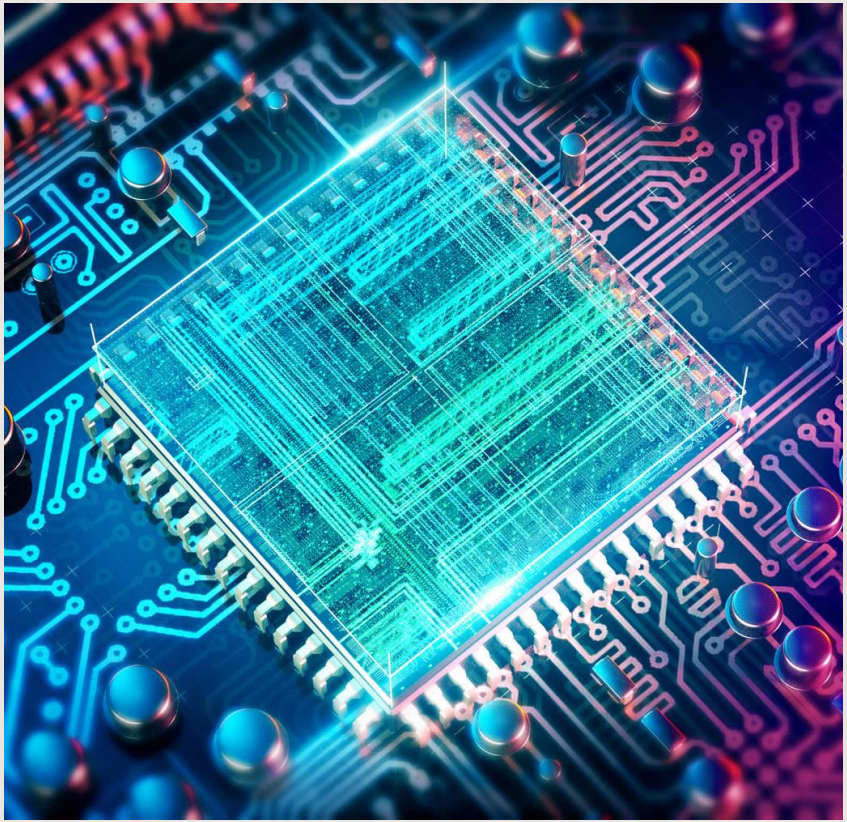
What will be discussed?



Hardware level



Hardware level



- Dump firmware
- Change firmware
- Get root terminal
- Get sensitive data
- Clonning device

Hardware level: Soldering Station

- Soldering iron
- Hot air gun
- Preheat station
- ~200$

Hardware level: Multimeter/Oscilloscope

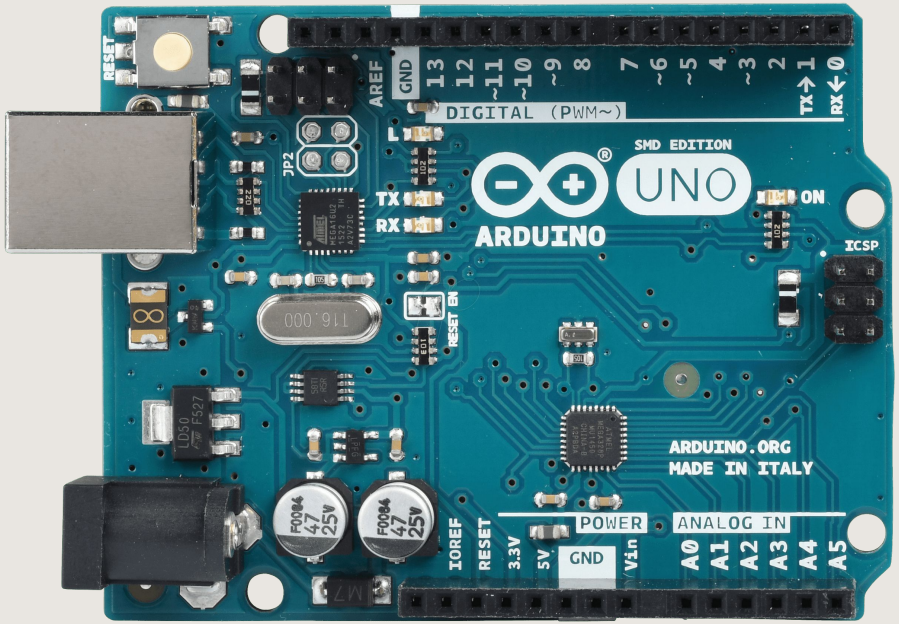
- Ammeter
- Voltmeter
- Ohmmeter
- Oscilloscope
- 45 - 95 $

Hardware level: logic analyzer

Hardware level: logic analyzer

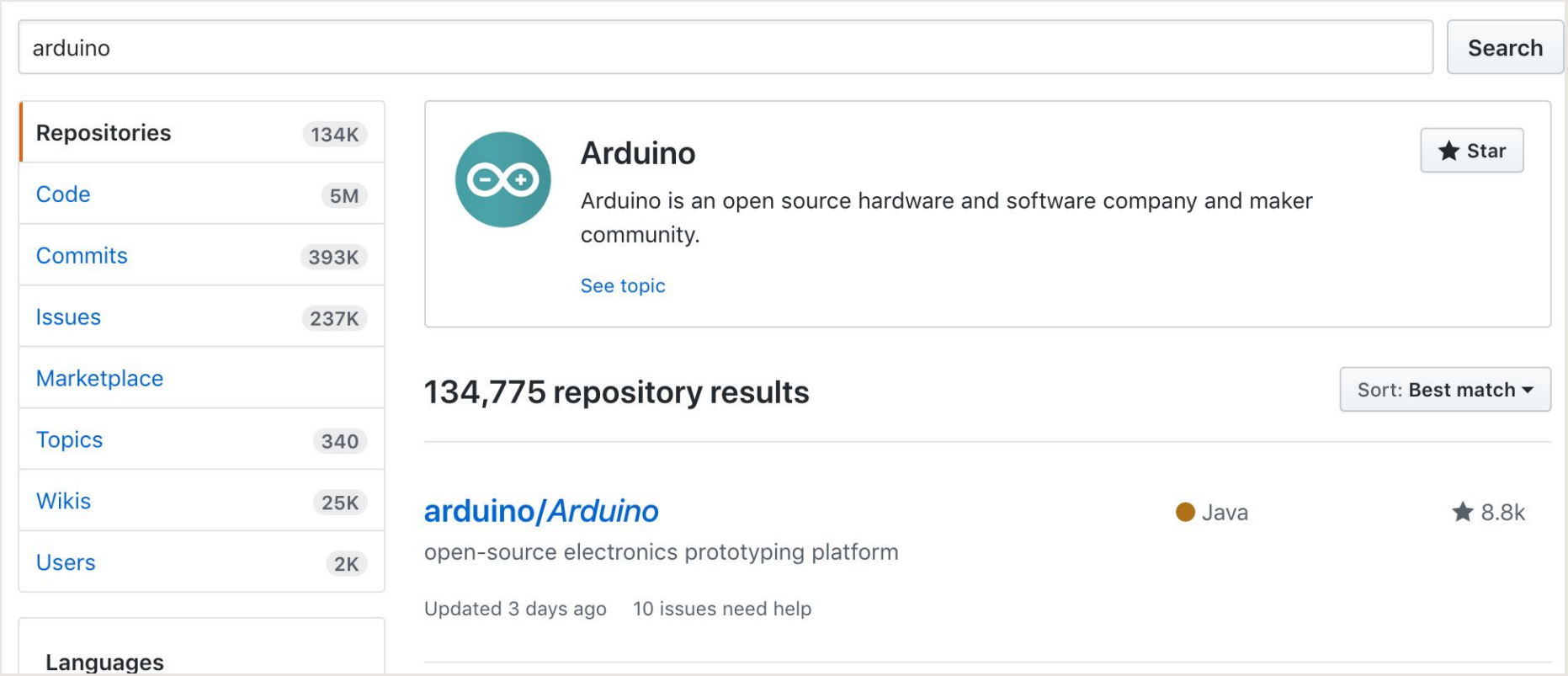
	Logic Pro 16	DSLogic
Inputs	16	16
Max Sample Rate	500 MS/s	400 MS/s
PC Connection	USB 3.0	USB 2.0
Price	1000$ (500$ for students)	150$

Hardware level: Arduino UNO

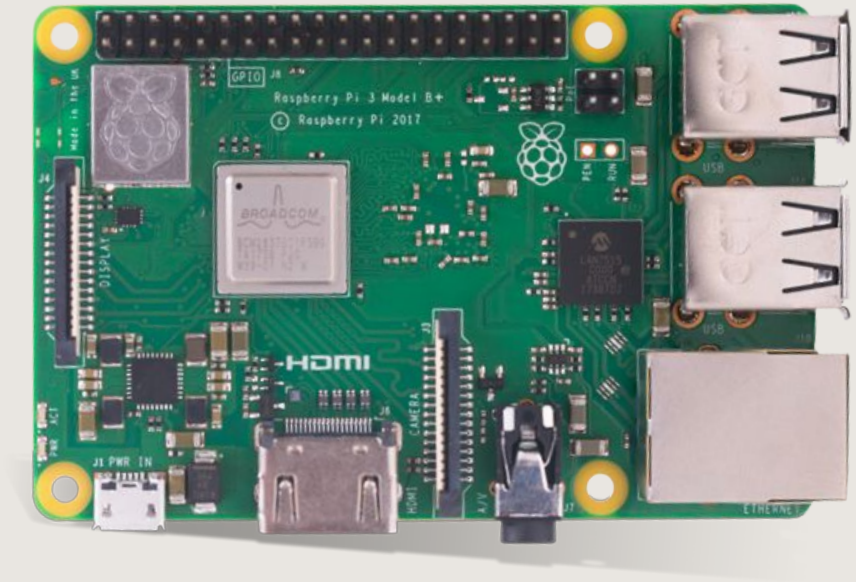


- 6 analog inputs
- 14 digital inputs
- Native USB <-> UART transceiver

Hardware level: Arduino UNO



Hardware level: Raspberry Pi



- 40 digital inputs
- Wi-Fi 802.11n
- Bluetooth 4.1

Hardware level: Raspberry Pi

Raspberry Pi | Search

- Repositories 53K
- Code 1M
- Commits 684K
- Issues 97K
- Marketplace
- Topics 106
- Wikis 19K
- Users 1K

Languages

Raspberry Pi ★ Star

The Raspberry Pi is a popular single-board computer.

See topic

53,816 repository results Sort: Best match

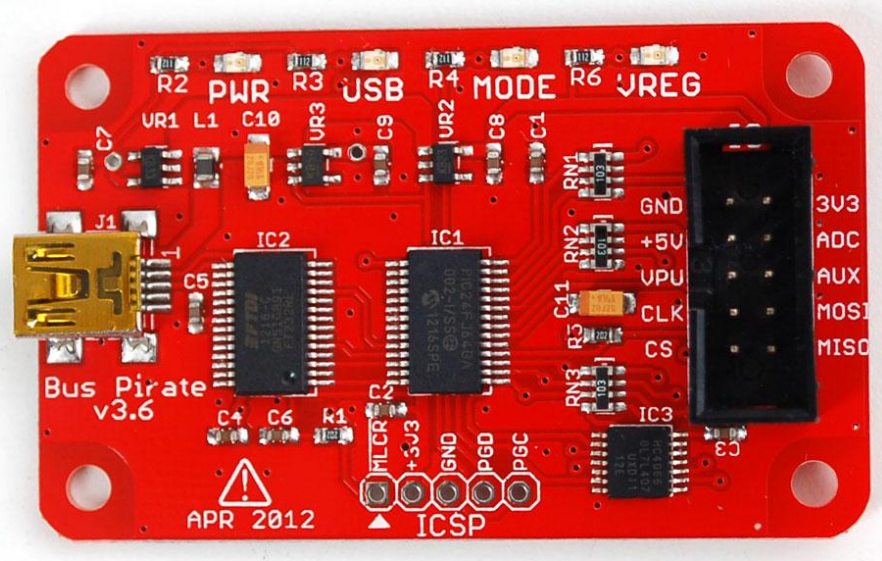
samjabrahams/tensorflow-on-*raspberry-pi* ● Python ★ 1.9k

TensorFlow for *Raspberry Pi*

tensorflow | raspberry-pi | machine-learning

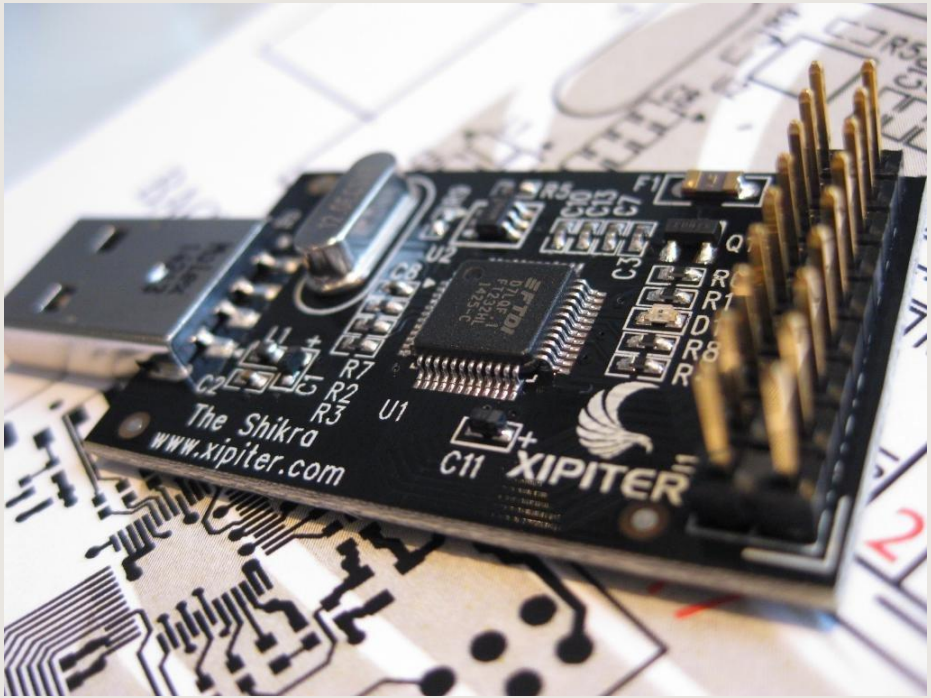
Updated on 8 Nov 2018

Hardware level: BusPirate



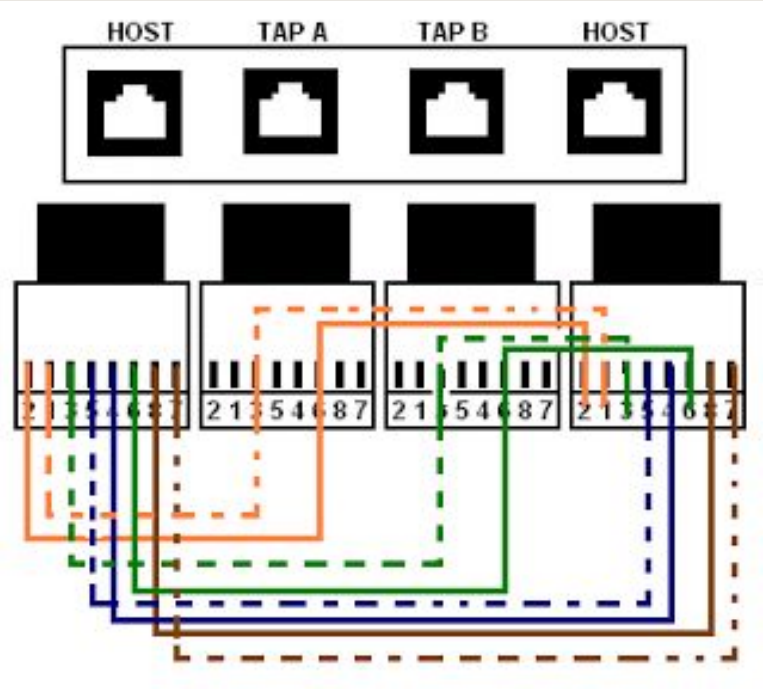
- Interfaces:
  - UART
  - JTAG
  - I2C
  - SPi
- Oscilloscope
- Logic Analyzer

Hardware level: The Shikra

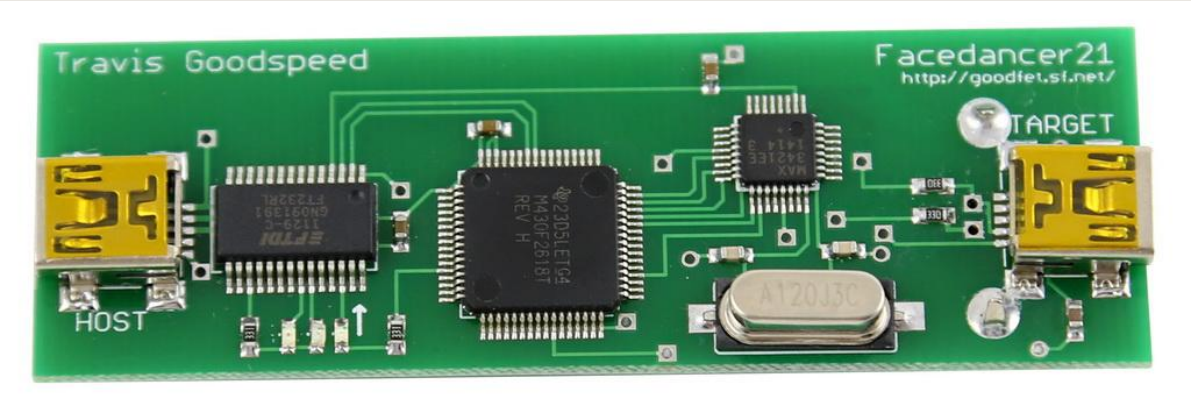


- Interfaces:
  - UART
  - JTAG
  - I2C
  - SPi
- The replacement of Buspirate

Hardware level: Lan Tap



Hardware level: Facedancer21



- Emulate any USB devices with Python lib.
  - Detect supported USB devices
  - Fuzz them
- Cost ~75$

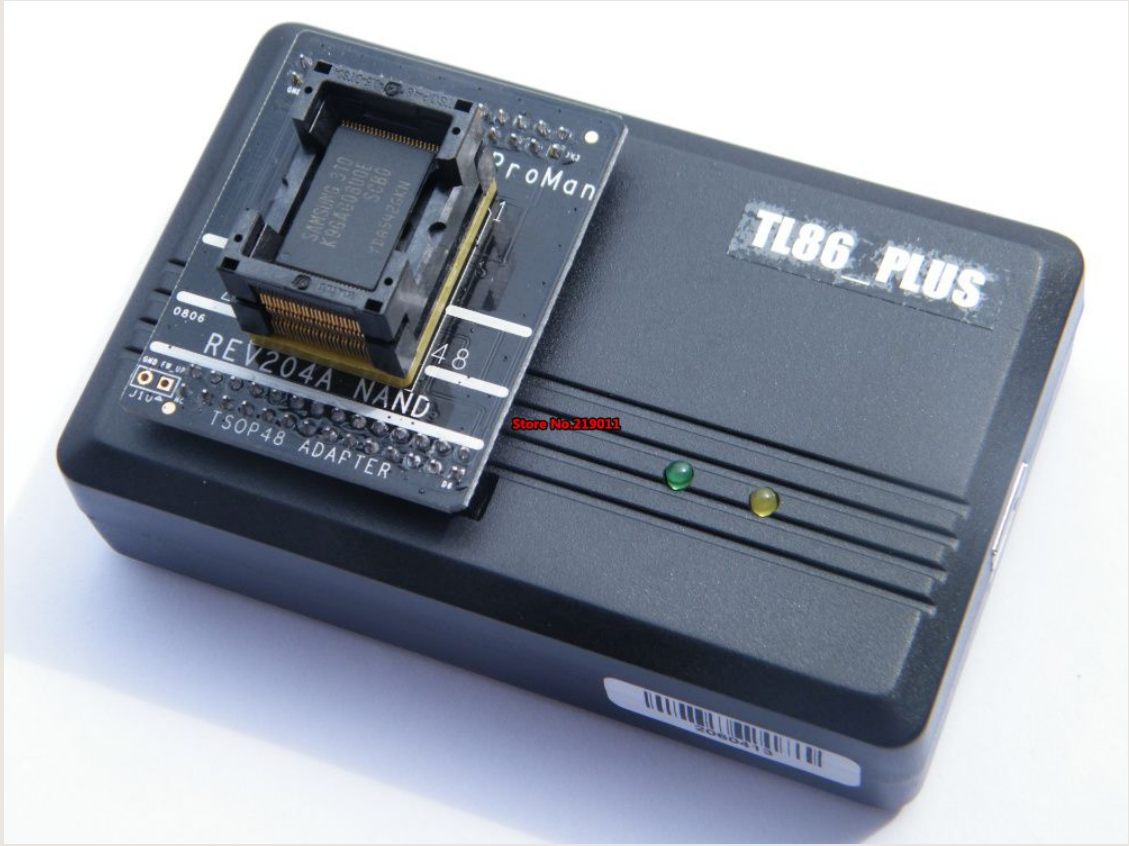
Hardware level: J-Link (China clone)

- Supported processor:
  - ARM7/9/11
  - Cortex-A5/A8/A9
  - Cortex-M0/M1/M3/M4
  - Cortex-R4
- SPI chip programming
- Debug options
- ~16$

Hardware level: TL866 Plus

- 24 memory adapters
- ~80$

Hardware level: TL86 Plus

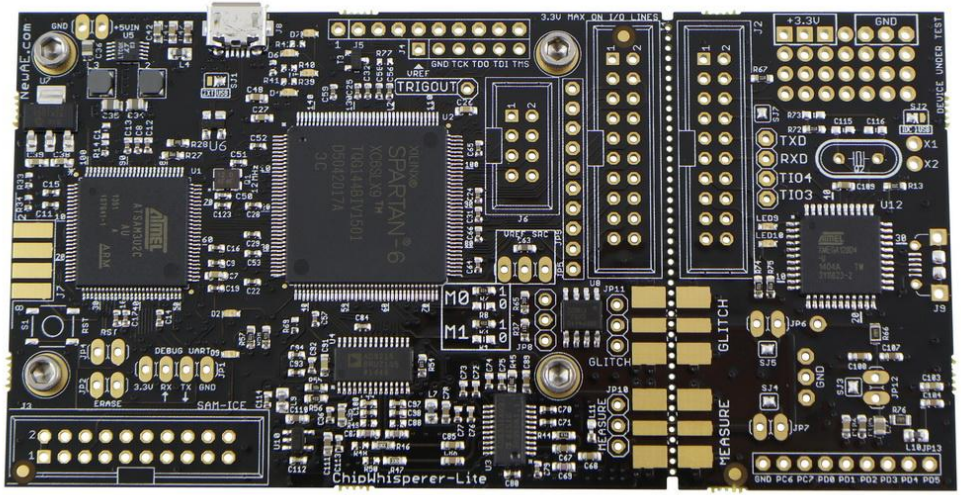


- Full NAND support
- ~80$

Hardware level: MOORC E-MATE X

- BGA memory support
- Memory to SD adapter
- ~100$

Hardware level: ChipWhisperer

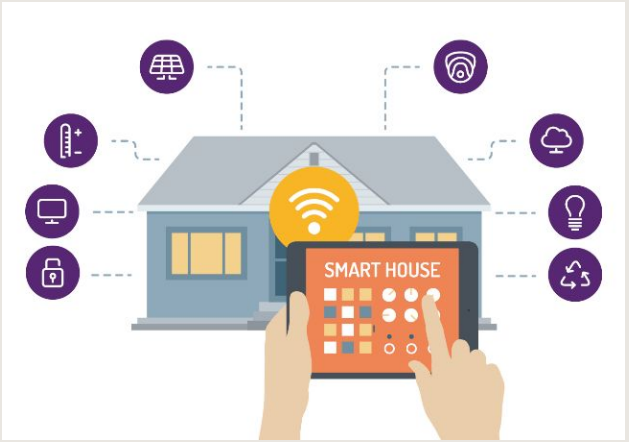


- clock glitching
- voltage glitching
- side-channel power analysis
- ~250$

Hardware level: ChipSHOUTER

- electromagnetic fault injection toolkit
- ~2800$

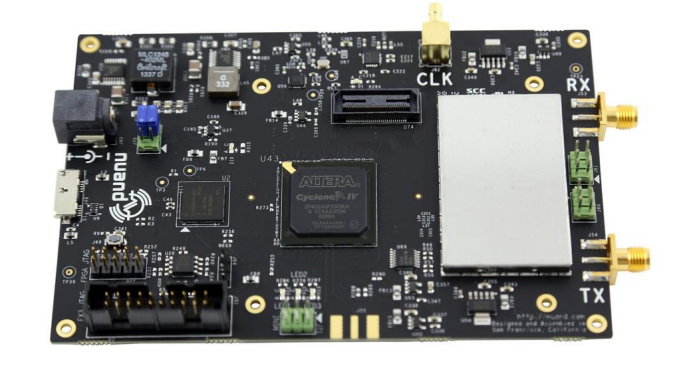
Radio level



Radio level: ALFA/TP-LINK WiFi adapters

- Monitoring mode
- Package injection
- 30$ - 80$

Radio level: HackRF, LimeSDR, BladeRF



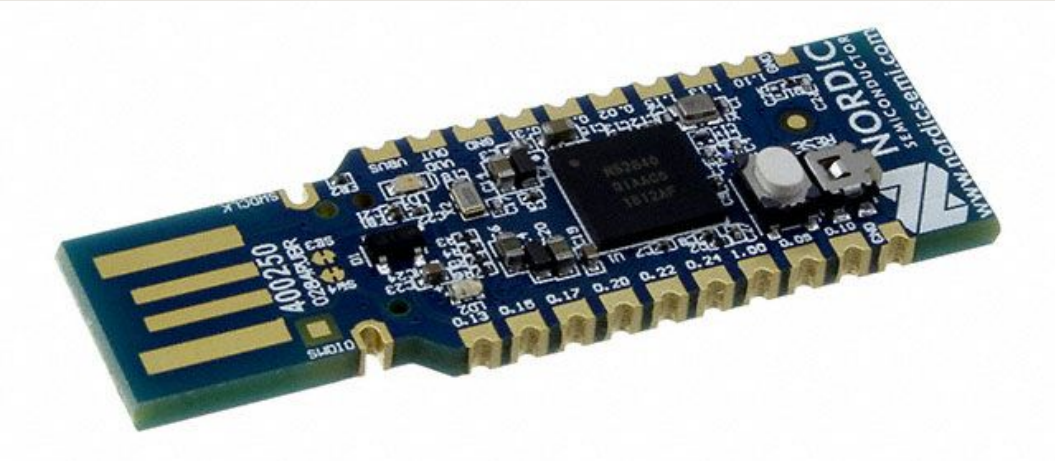
Radio level: HackRF, LimeSDR, BladeRF

	HackRF	BladeRF	LimeSDR
Frequency Range	1MHz-6GHz	300MHz-3.8GHz	100kHz-3.8GHz
RF Bandwidth	20MHz	40MHz	61.44MHz
Interface	USB 2.0	USB 3.0	USB 3.0
Duplex	Half	Full	Full
Price	300$	$420 ($650)	300$

Radio level: Ubertooth One

- Frequency hopping
- WireShark support
- BLE sniffer
- RubberDuck(???)
- 120$

Radio level: nrf52840 dongle



- BLE sniffer (including 5.0)
- Wireshark addon
- 18$

Radio level: CrazyRadio

- NRF24 demodulator
- Mousejack (???)
- 30$

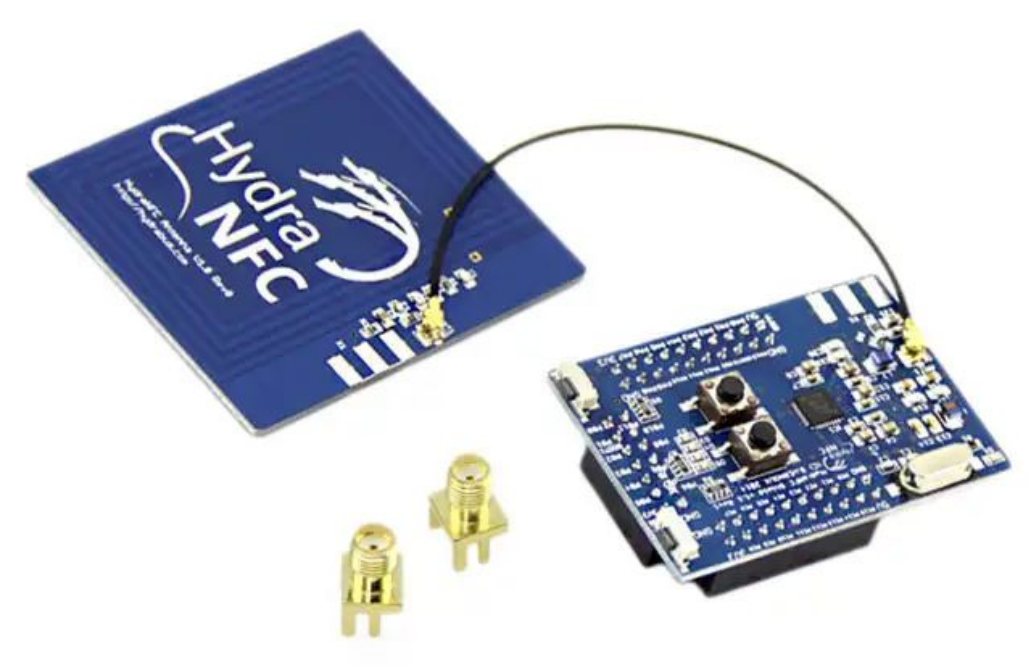
Radio level: ProxMark3

- NFC/RFID Card reader
- NFC Card emulator
- SmartCard support (?)
- ~60-300$

Radio level: ChameleonMini

- NFC/RFID Card reader
- NFC Card emulator
- ~75$

Radio level: HudraNFC(+HydraBus)



- NFC testing
- Raw ISO14443a/b sender
- 200$

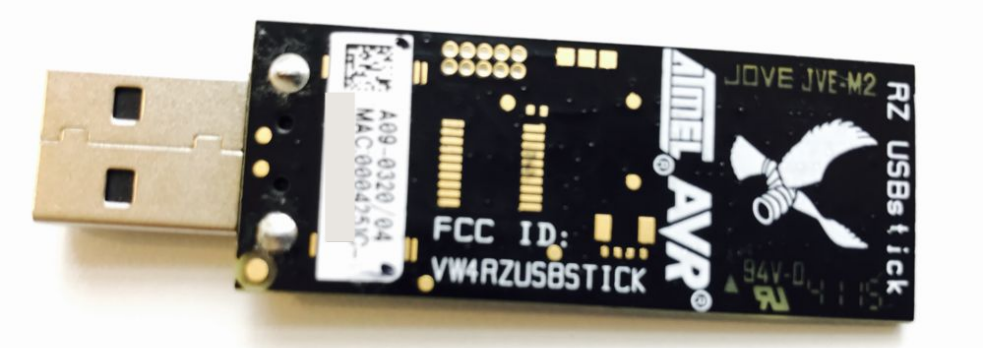
Radio level: MagSpoof

- 3-strip magnet card spoofer/emulator
- 65$

Radio level: UZB1

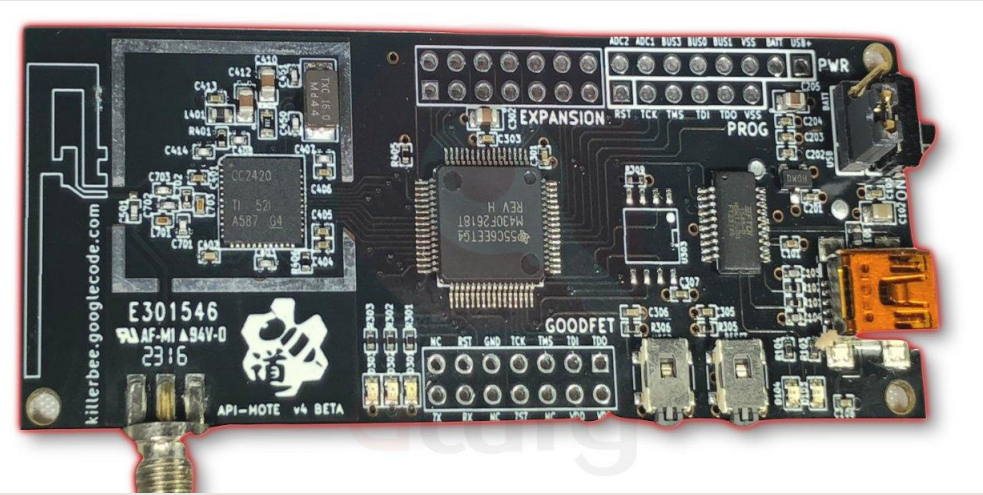
- Capture
- Transmit
- !!! US/EU Frequencies
- ~50$

Radio level: RZ Raven



- Capture
- Transmit
- KillerBee support
- ~120$ (???)

Radio level: APImote



- Capture
- Transmit
- KillerBee support
- ~150$

Questions?

Thanks 4 your attention :)

Telegram: @drakylar
Email: iljashaposhnikov@gmail.com

DEFCON NN