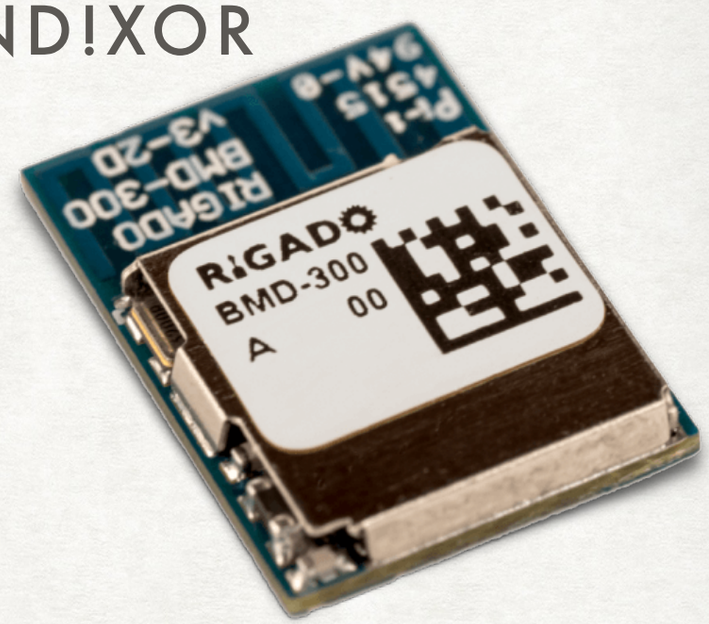
Paul (Skunkwrx)

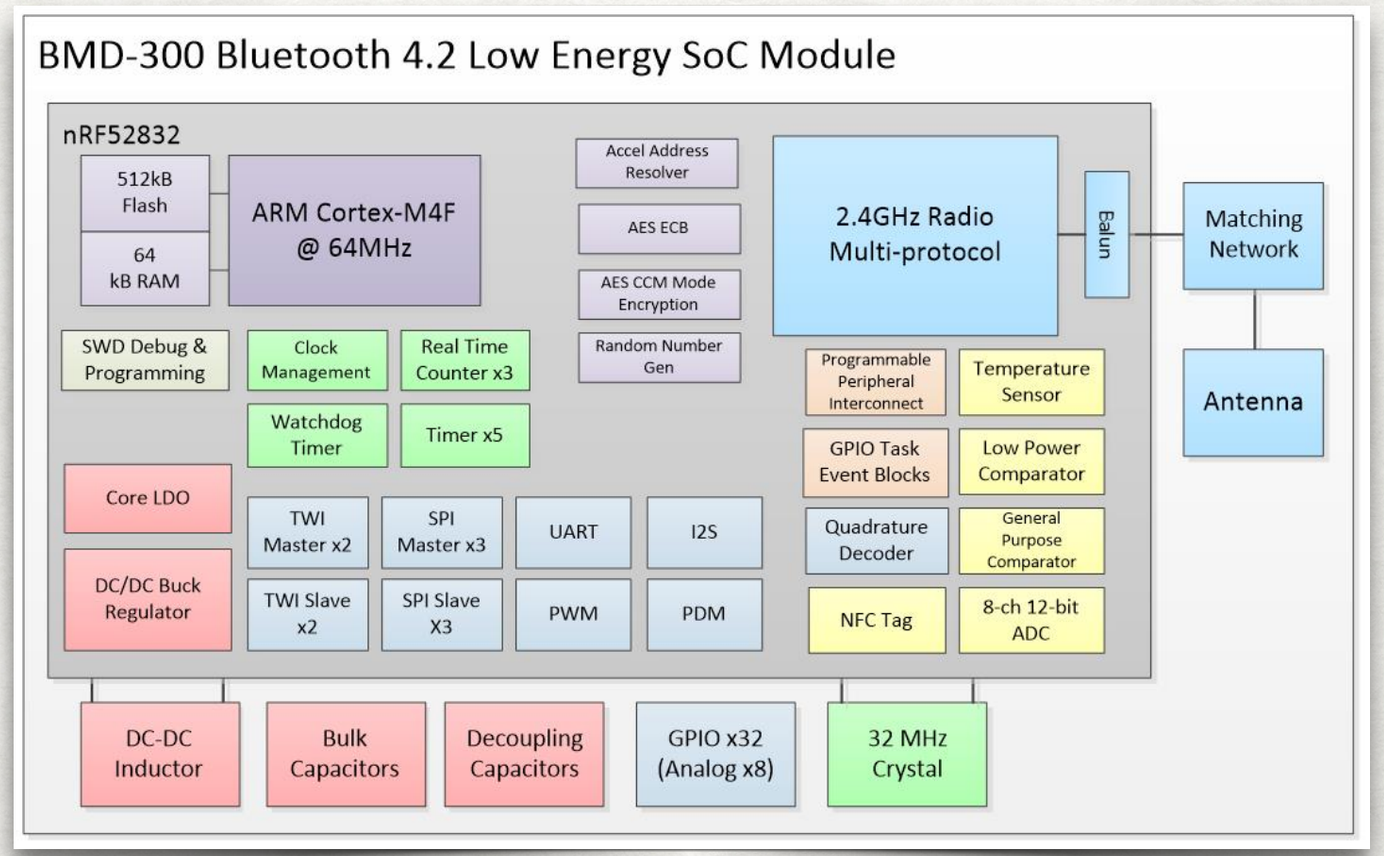
BASIC BLUETOOTH REVERSE ENGINEERING AND THE WALL OF BENDER

BENDER BADGE BLUETOOTH

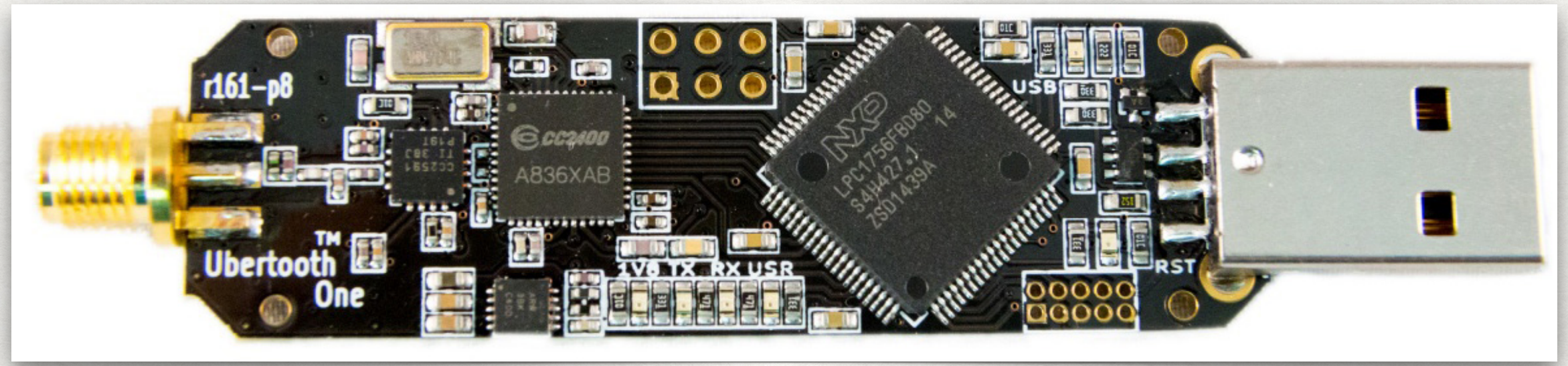
DEFCON 25 Unofficial Badge by AND!XOR



- Rigado BMD-300
  - Nordic nRF52832 BLE SoC
  - Bluetooth 4.2 compliant
  - 64 MHz ARM Cortex M4F
  - 512kB flash, 64kB RAM
  - Power management
  - Used by various badges at DEFCON

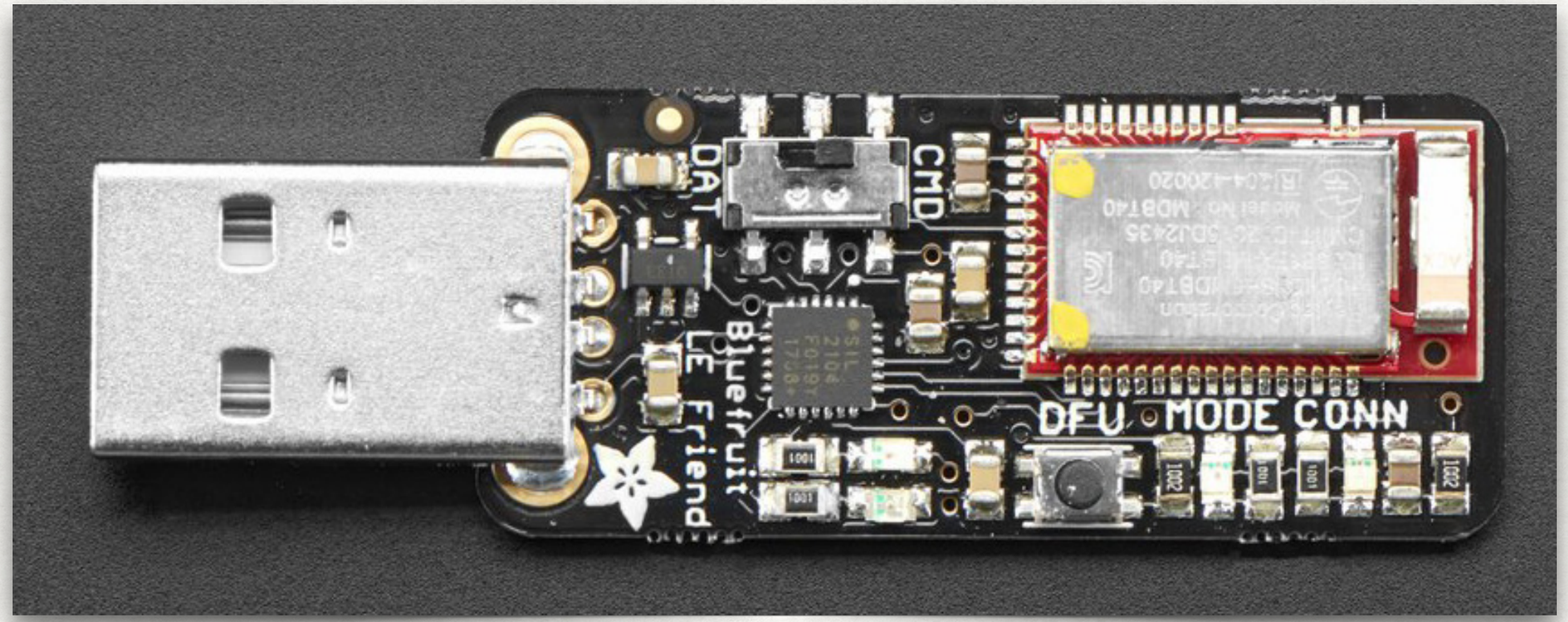


UBERTOOTH ONE



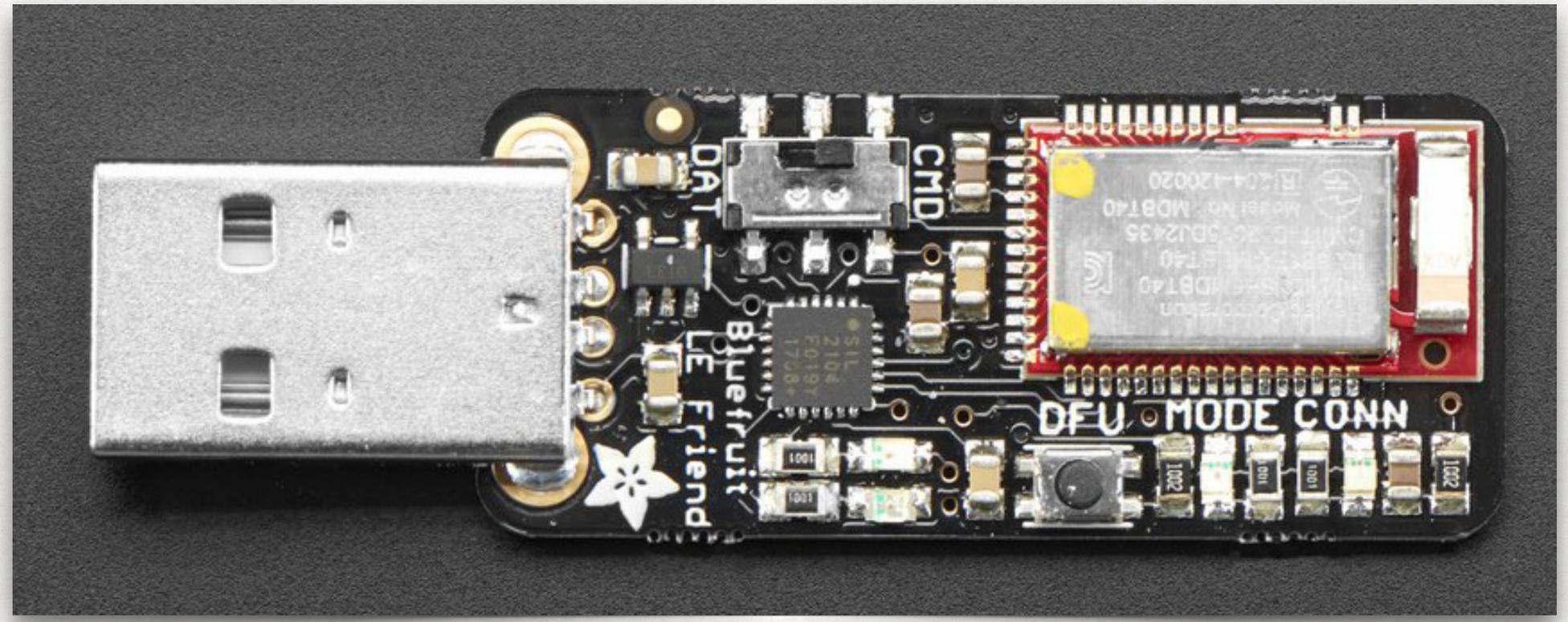
- Bluetooth Development Platform from Great Scott Gadgets
- $118 with matching RP-SMA antenna
- Transmit and receive
- https://github.com/greatscottgadgets/ubertooth
- Recommends Linux only, with a list of dependencies

BLUEFRUIT LE FRIEND



- Aimed at makers needing to interface with their own devices
- Supports BLE UART connections transparently
- Supports an AT command set to control GATT Services, Characteristics, and advertising beacons
- Easiest way to generate BLE advertisements (badge spoofing)

BLUEFRUIT LE SNIFFER



- Special firmware in a Bluefruit LE Friend
- Streams Bluetooth Low Energy packets to Wireshark (or a file)
- Wireshark support is obsolete and Windows-only!
- Easiest way to trace BLE activity (advertising OR connected)

CAPTURING AN ADVERTISEMENT

with the Bluefruit LE Sniffer and Wireshark

5823	1008.15857	Slave	Master	LE LL	63	8f340701000000000b021	SKUNKWRX	6620	ADV_IND
5824	1008.17558	Slave	Master	LE LL	63	8f340701000000000b021	SKUNKWRX	6620	ADV_IND
5825	1008.65632	Slave	Master	LE LL	63	8f340701000000000b021	SKUNKWRX	6620	ADV_IND

```
Frame 5825: 63 bytes on wire (504 bits), 63 bytes captured (504 bits) on interface 0
Nordic BLE sniffer meta
Bluetooth Low Energy Link Layer
  Access Address: 0x8e89bed6
  Packet Header: 0x2540 (PDU Type: ADV_IND, TxAdd=false, RxAdd=false)
  Advertising Address: cf:25:fe:d6:b5:fb (cf:25:fe:d6:b5:fb)
  Advertising Data
    Appearance: Unknown
      Length: 3
      Type: Appearance (0x19)
      Appearance: Unknown (0x19dc)
    Flags
    Manufacturer Specific
      Length: 13
      Type: Manufacturer Specific (0xff)
      Company ID: Unknown (0x049e)
      Data: 8f340701000000000b021
    Device Name: SKUNKWRX
      Length: 9
      Type: Device Name (0x09)
      Device Name: SKUNKWRX
CRC: 0xafadd1
```

COPYING AN ADVERTISEMENT

with the Bluefruit Friend LE

S K U N K W R X

AT+GAPSETADVDATA=03-19-DC-19-02-01-06-0D-FF-9E-04-AB-CD-06-00-00-00-00-00-B0-3E-09-09-53-4B-55-4E-4B-57-52-58

"Appearance"
0xDC19
or "DC 25"

Flags

Advertisement

Local Name

0D-FF-9E-04-AB-CD-06-00-00-00-00-00-B0-3E

Field Length 0x0D = 13 bytes

Type 0xFF == Manufacturer Specific Data

Badge ID

?????

1181	0x049D	Uhlmann & Zacher GmbH
1182	0x049E	AND!XOR LLC
1183	0x049F	tictote AB
1184	0x04A0	Vypin, LLC

Official Registry of Bluetooth Company Names

BlueZ

built into Linux distros

BlueZ provides support for the core Bluetooth layers and protocols. It is flexible, efficient and uses a modular implementation. It has many interesting features:

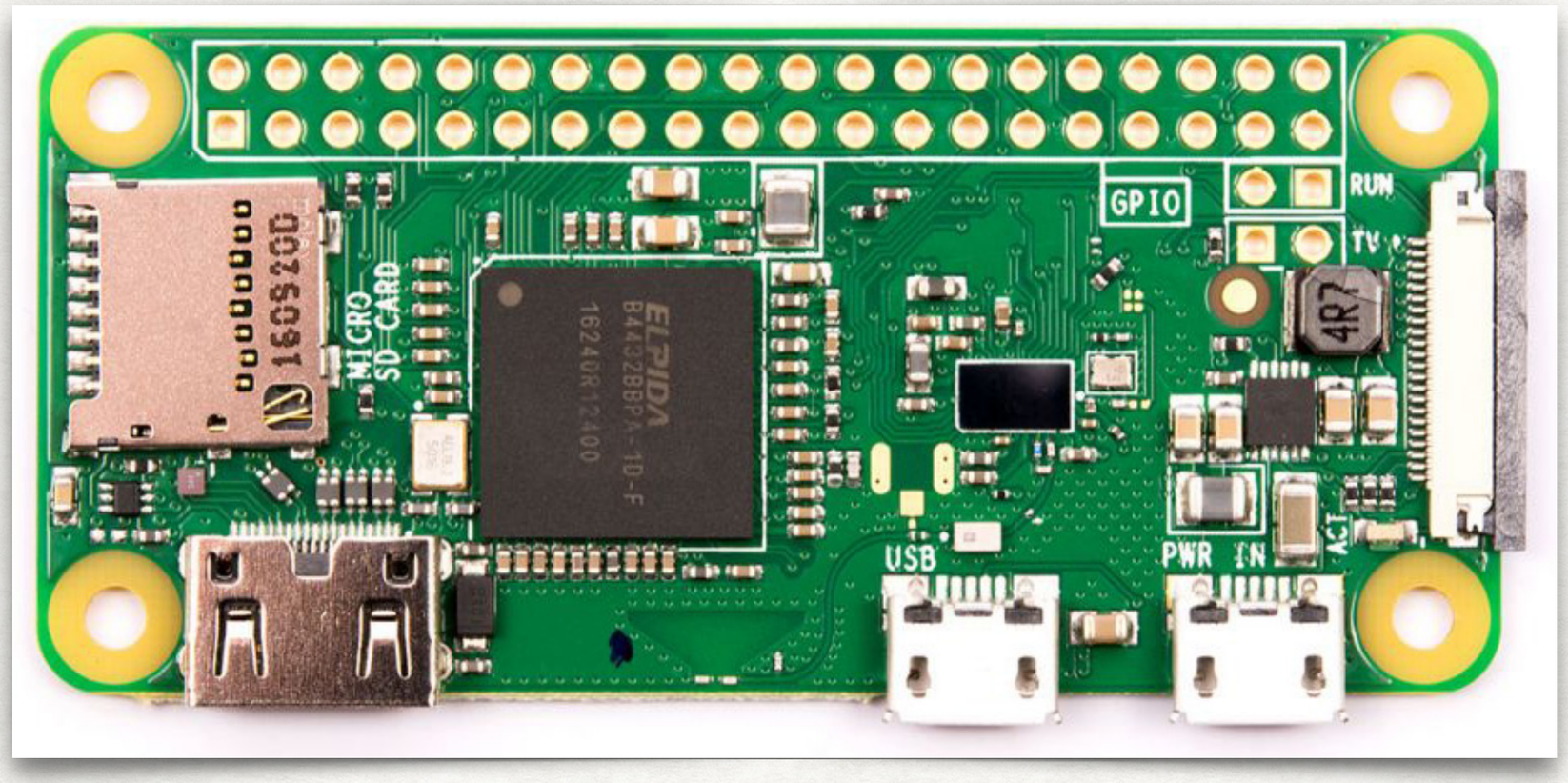
- Complete modular implementation
- Symmetric multi processing safe
- Multithreaded data processing
- Support for multiple Bluetooth devices
- Real hardware abstraction
- Standard socket interface to all layers
- Device and service level security support

Currently BlueZ consists of many separate modules:

- Bluetooth kernel subsystem core
- L2CAP and SCO audio kernel layers
- RFCOMM, BNEP, CMTP and HIDP kernel implementations
- HCI UART, USB, PCMCIA and virtual device drivers
- General Bluetooth and SDP libraries and daemons
- Configuration and testing utilities
- Protocol decoding and analysis tools

Raspberry Pi Zero W

it has built-in Bluetooth hardware!



- 1 GHz ARM with all the trimmings for $10
- Built-in Cypress CYW43438 for 802.11n WiFi and Bluetooth 4.0
- Standard Raspbian (Debian-derived) distro includes BlueZ support

WALL OF BENDER

or, what cool thing can we do with minimal understanding of how the badges interact via Bluetooth?

- Cheap hardware that could be left unattended:
  - Raspberry Pi Zero W with 8GB µSD card
  - LG HDMI LCD monitor, 1920p
  - HDMI cable
  - Wall wart and USB cable for USB power to Raspberry Pi
- 384 lines of Python code, some stolen from BlueZ example code
- Live on-screen display of Badge ID and Name info
- Logging of all badge advertisements to the µSD card